OpenManage Integration for VMware vCenter for Desktop Client

Benutzerhandbuch Version 2.3



Anmerkungen, Vorsichtshinweise und Warnungen

 **ANMERKUNG:** Eine ANMERKUNG liefert wichtige Informationen, mit denen Sie den Computer besser einsetzen können.

 **VORSICHT: Ein VORSICHTSHINWEIS macht darauf aufmerksam, dass bei Nichtbefolgung von Anweisungen eine Beschädigung der Hardware oder ein Verlust von Daten droht, und zeigt auf, wie derartige Probleme vermieden werden können.**

 **WARNUNG: Durch eine WARNUNG werden Sie auf Gefahrenquellen hingewiesen, die materielle Schäden, Verletzungen oder sogar den Tod von Personen zur Folge haben können.**

2015

Rev. A00

Inhaltsverzeichnis

1

Übersicht

OpenManage Integration for VMware vCenter

VMware vCenter ist die primäre von IT-Administratoren für die Verwaltung und Überwachung von VMware vSphere ESX/ESXi-Hosts verwendete Konsole. In einer virtualisierten Standardumgebung werden VMware-Warnungen und -Überwachungen verwendet, um einen Administrator für die Behebung von Hardware-Problemen zum Start einer separaten Konsole aufzufordern. Jetzt haben Administratoren mit OpenManage Integration for VMware vCenter neue Funktionen und Möglichkeiten, um die Dell-Hardware in der virtualisierten Umgebung zu verwalten und zu überwachen. Dazu gehören z. B.:

- Warnmeldungen und Umgebungsüberwachung
- Überwachung und Berichterstellung für Einzelserver
- Firmware-Aktualisierungen
- Erweiterte Bereitstellungsoptionen

Wichtige Funktionen

Dell-Kunden können OpenManage Integration for VMware vCenter zur Ausführung folgender Aufgaben verwenden:

Bestandsaufnahme	Bestandsaufnahme von wichtigen Ressourcen, Durchführen von Konfigurationsaufgaben sowie Bereitstellen von Cluster- und Datencenteransichten der Dell-Plattformen.
Überwachung und Warnmeldungen	Erkennen wichtiger Hardware-Fehler und Durchführen virtualisierungsbezogener Maßnahmen (zum Beispiel Migrieren von Arbeitslasten oder Versetzen von Hosts in den Wartungsmodus).
Firmware-Aktualisierungen	Aktualisieren von Dell-Hardware auf die aktuellste Version des BIOS und der Firmware.
Bereitstellung	Erstellen von Hardware- sowie Hypervisor-Profilen und Bereitstellen einer beliebigen Kombination dieser beiden auf Dell PowerEdge-Bare-Metal-Servern, remote und ohne PXE – mithilfe von vCenter.
Service-Informationen	Abrufen von Dell-Garantieinformationen aus dem Internet.

Wie hilft Ihnen die OpenManage Integration for VMware vCenter bei der vCenter-Verwaltung

OpenManage Integration for VMware vCenter enthält zusätzliche Virtualisierungsfunktionen, die die aktuellen vCenter-Verwaltungsfunktionen ergänzen:

- Es komprimiert Aufgaben und fügt Verwaltungsvorgänge wie Firmware-Aktualisierungen und Bare-Metal-Bereitstellung zur vCenter-Serververwaltungskonsole hinzu.
- Organisation der Bereitstellung von mehreren Bare-Metal-Servern, ohne dass eine PXE (Preboot Execution Environment) erforderlich ist.
- Bereitstellung zusätzlicher Daten (Bestand, Ereignisse, Alarme) zur Diagnose von Serverproblemen.
- Integration mit Standardauthentifizierung, -rollen und -berechtigungen von vCenter.

OpenManage Integration for VMware vCenter

Die folgenden Schritte sind allgemeine Funktionen von OpenManage Integration for VMware vCenter:

- Überwachung von Dell-Servern unter Verwendung des vCenter-Standardereignisses und -Alarm-Untersystems
- Durchführung erweiterter Hardware-Verwaltung und -Konfiguration
- Durchführung einer Zero-Touch-Bereitstellung von VMware ESX / ESXi-Hypervisoren auf Bare-Metal-Systemen ohne Verwendung von PXE
- Aufbau von Hardware und VMware ESX / ESXi-Hypervisor-Profilen
- Durchführung von Firmware-Aktualisierungen
- Behebung von Infrastrukturproblemen
- Berichterstattung in der Datencenter- und Cluster-Ansicht; Export in CSV-Datei
- Integration von OpenManage Integration for VMware vCenter-Funktionen mit standardmäßigen vCenter-Rollen und -Berechtigungen

2

OpenManage Integration for VMware vCenterKonfiguration

In den folgenden Abschnitten erhalten Sie schrittweise Anleitungen für dieOpenManage Integration for VMware vCenter- Erstkonfiguration. Informationen zu Aktualisierung, Deinstallation und zur Sicherheitsrolle werden ebenfalls in den folgenden Abschnitten behandelt.

Sicherheitsrollen und Berechtigungen

OpenManage Integration for VMware vCenterspeichert Benutzeranmeldeinformationen in einem verschlüsselten Format. Es liefert keine Kennwörter an Clientanwendungen, um nicht ordnungsgemäße Anforderungen zu vermeiden, die zu Problemen führen könnten. Die Datenbanksicherungen werden mithilfe benutzerdefinierter Sicherheitsausdrücke vollständig verschlüsselt, so dass die Daten nicht missbräuchlich verwendet werden können.

Standardmäßig verfügen Benutzer in der Gruppe der Administratoren über alle Berechtigungen. Administratoren können alle Funktionen von OpenManage Integration for VMware vCenter im VMware vCenter verwenden. Wenn Sie möchten, dass ein Nicht-Admin-Benutzer das Produkt verwaltet, dann erstellen Sie eine Rolle, die beide Dell-Rollen enthält, weisen Sie dann in der Bestandsliste auf dem root/übergeordneten (top)-Knoten eine Berechtigung zu und propagieren Sie Berechtigungen nach Bedarf auf die untergeordneten (child)-Knoten, für die Sie dem Benutzer Zugriff gewähren wollen. Zum Beispiel: Wenn Sie möchten, dass ein Benutzer nur Cluster A verwaltet, dann behalten Sie die Berechtigungen für Cluster A bei und entfernen Sie die Berechtigungen der anderen Cluster.

Datenintegrität

Die Kommunikation zwischen dem virtuellen Gerät des OpenManage Integration for VMware vCenter, der Verwaltungskonsole und vCenter erfolgt mithilfe von SSL/HTTPS. Das OpenManage Integration for VMware vCenter generiert ein SSL-Zertifikat, das für die vertrauenswürdige Kommunikation zwischen vCenter und dem Gerät verwendet wird. Es überprüft und vertraut außerdem dem Zertifikat des vCenter-Servers vor der Kommunikation und der OpenManage Integration for VMware vCenter-Registrierung. Die Registerkarte der OpenManage Integration for VMware vCenter-Konsole (in VMware Center) nutzt Sicherheitsverfahren, um unzulässige Anforderungen während der Übertragung von Schlüsseln von und auf die Verwaltungskonsole und Back-End-Services zu vermeiden. Bei diesem Sicherheitstyp schlagen gefälschte siteübergreifende Anforderungen fehl.

Eine sichere Verwaltungskonsolensitzung hat ein Leerlauf-Zeitlimit von fünf Minuten, und die Sitzung ist nur im aktuellen Browser-Fenster und/oder -Register gültig. Wenn der Benutzer versucht, die Sitzung in einem neuen Fenster oder Register zu öffnen, wird ein Sicherheitsfehler generiert, der eine gültige Sitzung anfordert. Durch diese Aktion wird auch verhindert, dass der Benutzer auf eine schädliche URL klickt, die die Verwaltungskonsolensitzung angreifen könnte.

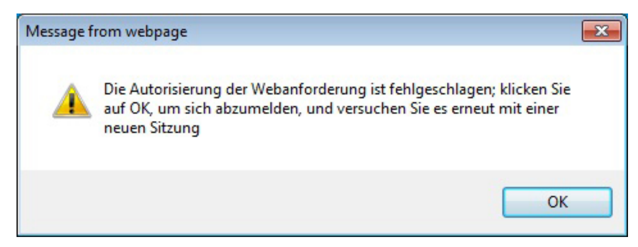


Abbildung 1. Fehlermeldung

Zugangskontrollenauthentifizierung, Autorisierung und Rollen

Das OpenManage Integration for VMware vCenter verwendet die aktuelle Benutzersitzung des vSphere Client und die gespeicherten Administrations-Anmeldeinformationen, damit das virtuelle Gerät vCenter-Operationen durchführen kann. Das OpenManage Integration for VMware vCenter nutzt die integrierten Rollen und das Berechtigungsmodell des vCenter-Servers, um Benutzeraktionen mit dem virtuellen Gerät und den verwalteten vCenter-Objekten (Hosts und Clusters) zu authorisieren.

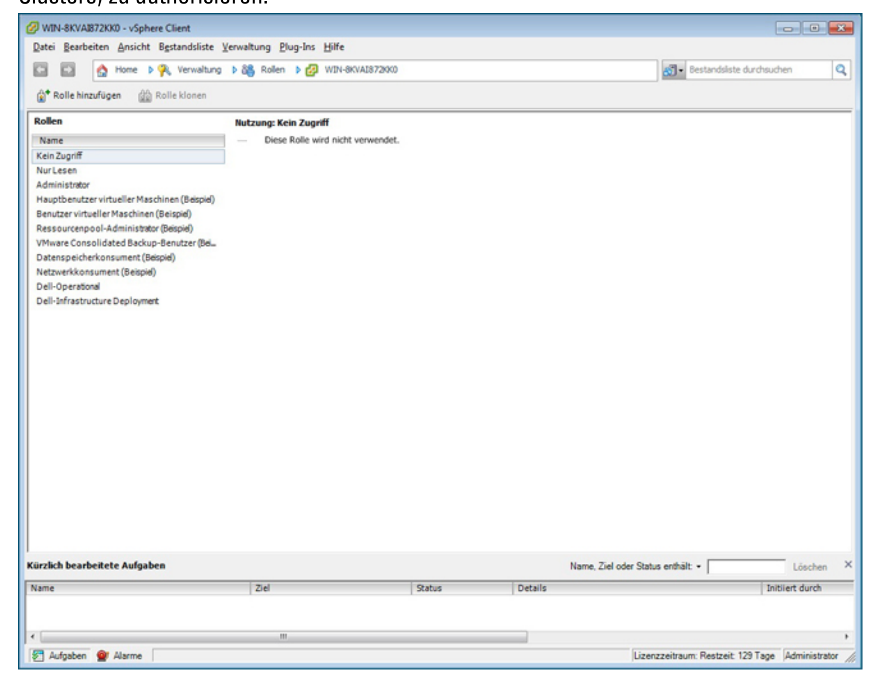


Abbildung 2. Rollen und Berechtigungen des vSphere-Client auf vCenter

Dell-Vorgangsrolle

Enthält die Berechtigungen/Gruppen zur Ausführung von Geräte- und vCenter Server-Aufgaben einschließlich Firmware-Aktualisierungen, Hardware-Bestandslisten, Neustarten eines Hosts, Versetzen eines Hosts in den Wartungsmodus oder Erstellen einer vCenter Server-Aufgabe

Diese Rolle umfasst die folgenden Berechtigungsgruppen.

Berechtigungsgruppe – Dell.Konfiguration Berechtigung – Ausführen von mit Hosts verknüpften Aufgaben, Ausführen von mit vCenter verknüpften Aufgaben, Konfigurieren von SelLog, Konfigurieren von ConnectionProfile, Konfigurieren von ClearLed, Firmware-Aktualisierung

Berechtigungsgruppe – Dell.Bestandsaufnahme	Berechtigung – Konfigurieren der Bestandsaufnahme, Konfigurieren des Garantieabrufs, Konfigurieren von ReadOnly
Berechtigungsgruppe – Dell.Überwachung	Berechtigung – Konfigurieren der Überwachung, Überwachen
Berechtigungsgruppe – Dell.Berichterstellung (nicht verwendet)	Berechtigung – Erstellen eines Berichts, Ausführen eines Berichts

Dell-Infrastrukturbereitstellungsrolle

Diese Rolle umfasst die Berechtigungen, die besonders mit den Hypervisor-Bereitstellungsfunktionen verknüpft sind.

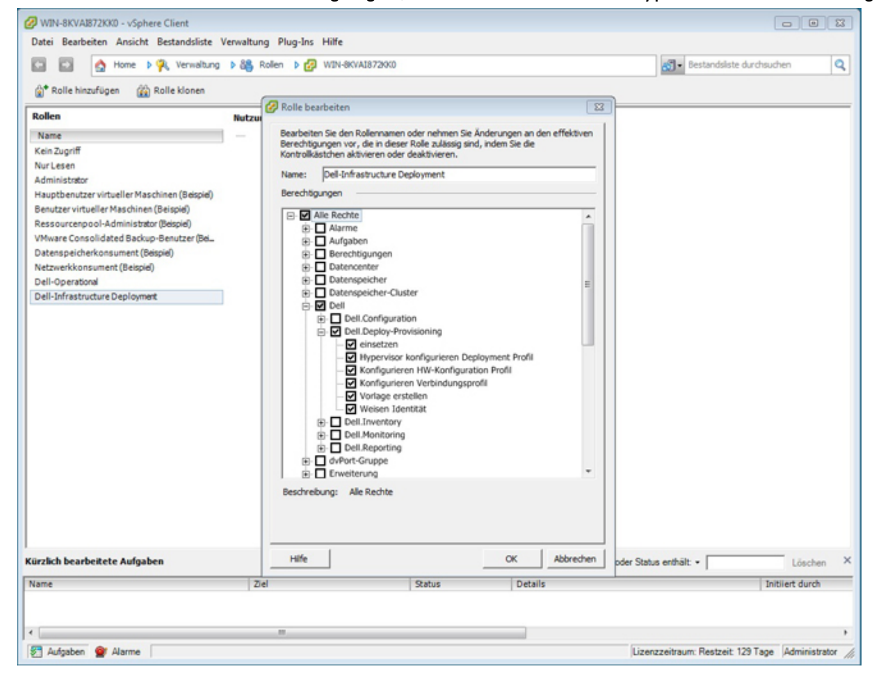


Abbildung 3. Dell-Infrastrukturbereitstellungsrolle

Die von dieser Rolle gewährten Berechtigungen sind „Vorlage erstellen“, „HW-Konfigurationsprofil konfigurieren“, „Hypervisor-Bereitstellungsprofil konfigurieren“, „Verbindungsprofil konfigurieren“, „Identität zuweisen“ und „Bereitstellen“.

Dell.Deploy – Bereitstellung	Erstellen von Vorlagen, Konfigurieren des HW-Konfigurationsprofils, Konfigurieren des Hypervisor-Bereitstellungsprofils, Konfigurieren des Verbindungsprofils, Zuweisen einer Identität, Bereitstellen

Grundlegende Informationen zu Berechtigungen

Jede vom OpenManage Integration for VMware vCenter ausgeführte Aktion ist einer Berechtigung zugeordnet. In den folgenden Abschnitten werden die verfügbaren Aktionen und die zugeordneten Berechtigungen aufgeführt:

- Dell.Konfiguration.Ausführen von mit vCenter verknüpften Aufgaben
  - Beenden und Starten des Wartungsmodus
  - Aufrufen der vCenter-Benutzergruppe zur Abfrage von Berechtigungen
  - Registrieren und Konfigurieren von Warnungen, z. B. Aktivieren/Deaktivieren von Warnungen auf der Seite mit den Ereigniseinstellungen
  - Veröffentlichen von Ereignissen/Warnungen bei vCenter
  - Konfigurieren von Ereigniseinstellungen auf der Seite mit den Ereigniseinstellungen
  - Wiederherstellen von Standardwarnungen auf der Seite mit den Ereigniseinstellungen
  - Überprüfen des DRS-Status auf Clustern während der Konfiguration von Warnungs-/Ereigniseinstellungen
  - Neustarten des Hosts nach Aktualisierungs- oder anderen Konfigurationsmaßnahmen
  - Überwachen des Status/Fortschritts von vCenter-Tasks
  - Erstellen von vCenter-Tasks, z. B. Firmware-Aktualisierungstask, Hostkonfigurationstask und Bestandsaufnahmetask
  - Aktualisieren des Status/Fortschritts von vCenter-Tasks
  - Abrufen von Hostprofilen
  - Hinzufügen von Hosts zu einem Datencenter
  - Hinzufügen von Hosts zu einem Cluster
  - Übernehmen des Profils für einen Host
  - Abrufen von CIM-Anmeldeinformationen
  - Konfigurieren von Hosts für Konformität
  - Abrufen des Status des Konformitätstasks
- Dell.Bestandsaufnahme.Konfigurieren von ReadOnly
  - Abrufen aller vCenter-Hosts zum Aufbau der vCenter-Struktur während der Konfiguration von Verbindungsprofilen
  - Bei Auswahl der Registerkarte überprüfen, ob der Host ein Dell-Server ist
  - Abrufen der Adresse/IP von vCenter
  - Abrufen der Host-IP/Adresse
  - Abrufen des Benutzers der aktuellen vCenter-Sitzung basierend auf der vSphere-Clientsitzungs-ID
  - Abrufen der vCenter-Bestandsaufnahmestruktur, um die vCenter-Bestandsliste in einer Baumstruktur anzuzeigen.
- Dell.Überwachung.Überwachen
  - Abrufen des Hostnamens für die Veröffentlichung des Ereignisses
  - Ausführen von Ereignisprotokollierungsvorgängen, z. B. Aufrufen der Ereignisanzahl oder Ändern der Ereignisprotokolleinstellungen
  - Registrieren, Aufheben der Registrierung und Konfigurieren von Ereignissen/Warnungen – Empfangen von SNMP-Traps und Veröffentlichen von Ereignissen
- Dell.Konfiguration.Firmware-Aktualisierung
  - Ausführen einer Firmware-Aktualisierung

- Laden von Firmware-Repository- und DUP-Dateninformationen auf der Seite des Assistenten zur Firmware-Aktualisierung
  - Abfragen der Firmware-Bestandsliste
  - Konfigurieren der Firmware-Repository-Einstellungen
  - Konfigurieren des Stagingordners und Ausführen der Aktualisierung unter Verwendung der Stagingfunktion
  - Testen der Netzwerk- und Repository-Verbindungen
- Dell.Bereitstellung-Bereitstellen.Erstellen von Vorlagen
  - Erstellen, Anzeigen, Löschen und Bearbeiten der Bereitstellungsvorlagen
- Dell.Konfiguration.Ausführen von mit Hosts verknüpften Tasks
  - Blink-LED, Lösch-LED, Konfigurieren der OMSA-URL von der Registerkarte zur Dell-Serververwaltung
  - Starten der OMSA-Konsole
  - Starten der iDRAC-Konsole
  - Anzeigen und Löschen des SEL-Protokolls
- Dell.Bestandsaufnahme.Konfigurieren der Bestandsaufnahme
  - Anzeigen der Systembestandsliste auf der Registerkarte zur Dell-Serververwaltung
  - Abrufen von Speicherdetails
  - Abrufen von Stromüberwachungsdetails
  - Erstellen, Anzeigen, Bearbeiten, Löschen und Testen von Verbindungsprofilen auf der Seite mit den Verbindungsprofilen
  - Planen, Aktualisieren und Löschen des Bestandsaufnahmezeitplans
  - Ausführen einer Bestandsaufnahme auf Hosts

3

Wie OpenManage Integration for VMware vCenter konfiguriert oder bearbeitet werden kann

Nachdem Sie die grundlegende Installation der OpenManage Integration for VMware vCenter beenden, können Sie mit der Konfiguration des Geräts mithilfe einer der folgenden Methoden fortfahren, die weiter hinten in diesem Abschnitt beschrieben sind:

- **Konfigurationstasks im Konfigurationsassistenten**
- **Konfigurationstasks mithilfe der Einstellungsoptionen**

Obwohl der Einsatz des Konfigurationsassistenten die am häufigsten verwendete Methode ist, können Sie diese Aufgabe auch über die Einstellungsseite des Geräts im Dell Management Center durchführen.

Die Benutzeroberfläche ist in beiden Bereichen ähnlich. Im Assistenten klicken Sie auf die Schaltfläche *Speichern und fortfahren* während Sie auf der Seite „Einstellungen" auf *Anwenden* klicken.

Konfigurationstasks im Konfigurationsassistenten

Verwenden Sie diese Konfigurationstasks, wenn Sie die OpenManage Integration for VMware vCenter unter Verwendung des Konfigurationsassistenten konfigurieren:

1. Willkommens-Seite im Konfigurationsassistent
2. Erstellen eines neuen Verbindungsprofils
3. Konfigurieren von Ereignissen und Alarmen
4. Einrichten eines Proxyservers
5. Planen von Bestandsaufnahme-Jobs
6. Ausführen eines Garantieabfrage-Jobs
7. Konfigurieren der Anmeldeinformationen für die Bereitstellung
8. Einrichten eines Standard-Repositorys für Firmware-Aktualisierungen
9. Aktivieren des OMSA-Links

Konfigurationstasks mithilfe der Einstellungsoptionen

Verwenden Sie diese Tasks zum Einrichten oder Bearbeiten der OpenManage Integration for VMware vCenter-Konfigurations-Tasks:

- Erstellen eines neuen Verbindungsprofils
- Konfigurieren von Ereignissen und Alarmen
- Einrichten eines Proxyservers
- Modifizieren eines Zeitplans zum Erstellen einer Bestandsaufnahme
- Garantieabfrage
- Anzeigen bzw. Bearbeiten der Anmeldeinformationen für die Bereitstellung
- Einrichten des Firmware-Repositorys und der Anmeldeinformationen

- Aktivieren des OMSA-Links

OpenManage Integration for VMware vCenter-Startseite

Wenn Sie sich bei der OpenManage Integration for VMware vCenter Startseite anmelden, befinden sich die Navigationsschaltflächen im linken Fensterbereich. Der rechte Fensterbereich enthält nützliche Links und weiterführende Informationen. Dieses Design bietet die wichtigsten Links zu den am häufigsten ausgeführten Aufgaben. Alle diese Aufgaben befinden sich im linken Fensterbereich. Sie finden sie auch auf der Startseite zur leichteren Verwendung. Die auf dieser Seite verfügbaren Aufgaben gehören zu den folgenden Kategorien:

- Host- und Server-Bereitstellung

  Dieser Abschnitt bietet weitere Informationen zur Host- und Server-Bereitstellung.
- vSphere-Host- und Bare-Metal-Server-Konformität

  Dieser Abschnitt enthält weiterführende Informationen und ermöglicht es Ihnen, Details zu nicht konformen Hosts oder Bare-Metal-Servern anzuzeigen oder die Assistenten auszuführen, um die Fehler zu korrigieren.
- Bestandsaufnahmezeitplan

  In diesem Abschnitt erfahren Sie mehr über die Zeitpläne zum Erstellen von Bestandslisten.
- Zeitplan für Garantieabfragen

  In diesem Abschnitt erfahren Sie mehr über das Anzeigen/Ändern von Garantieplänen.
- Lizenzierung

  In diesem Abschnitt erfahren Sie mehr über die Lizenzierung. Verwenden Sie die Links, um zu den Lizenzierungstasks zu gelangen.
- Ereignisse und Alarmeinstellungen

  Hier finden Sie Informationen zu den Ereignis- und Alarmeinstellungen oder können auf einen Link klicken, um diese Einstellungen zu konfigurieren.
- Hostverbindungslizenzen

  Hier können Sie die Hostverbindungslizenzen in Echtzeit anzeigen. Darüber hinaus können Sie auf den Link „Jetzt kaufen" klicken, um eine Lizenz für die Vollversion zu erwerben, so dass Sie mehrere Hosts verwalten können. Der Link „Jetzt kaufen" wird nur dann angezeigt, wenn Sie eine Demolizenz verwenden.
- vCenter-Verbindungslizenzen. Hier können Sie Informationen in Bezug auf die VMware vCenter-Verbindungslizenz anzeigen. Weitere Informationen zur vCenter-Verbindungslizenz finden Sie unter Informationen zur Lizenzierung für OpenManage Integration for VMware vCenter

Willkommens-Seite im Konfigurationsassistent

Nach der Installation der OpenManage Integration for VMware vCenter muss sie konfiguriert werden.

1. Klicken Sie im **vSphere-Client** auf der **Start**seite unter Registerkarte **Verwaltung** auf das Symbol **Dell Management Center** .
2. Wenn Sie das erste Mal auf das Symbol **Dell Management Center** klicken, wird der **Konfigurationsassistent** angezeigt. Sie können auf diesen Assistenten auch über die Seite **Dell Management Center** → **Einstellungen** zugreifen.
3. Überprüfen Sie auf der Registerkarte **Willkommen** die gewählten Schritte und klicken Sie dann auf **Weiter**.

Erstellen eines neuen Verbindungsprofils [Assistent]

Ein Verbindungsprofil speichert die Anmeldeinformationen, die das virtuelle Gerät für die Kommunikation mit Dell Servern verwendet. Jeder Dell Server muss einem Verbindungsprofil zugeordnet sein, damit er vom Dell Management

Plug-in verwaltet werden kann. Sie können mehrere Server zu einem Verbindungsprofil zuweisen. Das Verfahren zum Erstellen des Verbindungsprofils ist im Konfigurationsassistenten und im Dell Management Center, Option „Einstellungen“ nahezu identisch.

 **ANMERKUNG:** Bei Installationen auf Hosts mit Dell PowerEdge-Servern ab der 12. Generation ist die Installation des OMSA-Agenten nicht erforderlich. Bei Installationen auf Servern der 11. Generation wird der OMSA-Agent jetzt automatisch vor dem Bereitstellungsprozess installiert.

So erstellen Sie ein neues Verbindungsprofil mithilfe des Assistenten:

1. Klicken Sie auf der Registerkarte **Verbindungsprofile** auf **Neu erstellen**.
2. Geben Sie im Fensterbereich **Profilname und Beschreibung** den **Profilnamen** und optional eine **Beschreibung** ein, die dabei helfen, benutzerdefinierte Verbindungsprofil zu verwalten. Klicken Sie dann auf **Weiter**
3. Wählen Sie im Fensterbereich **Zugewiesene Hosts** die Hosts für das Verbindungsprofil aus und klicken Sie auf **Weiter**.
4. Zeigen Sie die Anmeldeinformationen und die Verbindungsprotokolle an und klicken Sie auf **Weiter**.
5. Geben Sie die **iDRAC-Anmeldeinformationen** in den Fensterbereich „iDRAC“ ein.
   a. Geben Sie **Benutzername**, **Kennwort** und **Kennwort bestätigen** ein. Der Benutzername kann aus bis zu 16 Zeichen einschließlich White-Spaces bestehen. Die Kennwörter müssen identisch sein und dürfen nur druckbare ASCII-Zeichen umfassen.

       **ANMERKUNG:** Kennwörter dürfen bis zu 20 druckbare ASCII-Zeichen enthalten. Der Domainname darf alphanumerische Zeichen, nur - (Bindestrich) oder . (Punkt), enthalten.

   b. Unter **Zertifikatsprüfung** wählen Sie **Aktivieren**, um das iDRAC-Zertifikat herunterzuladen, zu speichern und für alle künftigen Verbindungen zu validieren, oder wählen Sie **Deaktivieren**, um keine Prüfung durchzuführen und das Zertifikat nicht zu speichern.

      Wenn Sie Active Directory verwenden, müssen Sie „Aktivieren“ auswählen.
6. Klicken Sie auf **Weiter**.
7. Führen Sie im Fensterbereich **Anmeldeinformationen für das Host-Root** die folgenden Schritte aus:
   a. Geben Sie die entsprechenden Werte in die Felder **Benutzername**, **Kennwort** und **Kennwort bestätigen** ein. Die Kennwörter müssen identisch sein.

       **ANMERKUNG:** Kennwörter dürfen nicht mehr als 127 Zeichen umfassen und keine Sonderzeichen enthalten.

       **ANMERKUNG:** Bei Servern, die nicht über eine iDRAC Express- oder iDRAC-Enterprise-Karte verfügen, wenn der iDRAC-Verbindungstest ausgeführt wird, wird die Meldung *Für dieses System nicht anwendbar* angezeigt.

      ANMERKUNG: Die OMSA-Anmeldeinformationen sind die gleichen, die auch für ESX- und ESXi-Hosts verwendet werden.

   b. Unter **Zertifikatsprüfung** wählen Sie **Aktivieren**, um das OMSA-Zertifikat herunterzuladen, zu speichern und für alle künftigen Verbindungen zu validieren, oder wählen Sie **Deaktivieren**, um keine Prüfung durchzuführen und das Zertifikat nicht zu speichern. Wenn Sie Active Directory verwenden, müssen Sie „Aktivieren“ auswählen.
8. Klicken Sie auf **Weiter**.
9. Im Fenster **Verbindung testen** werden die eingegebenen iDRAC- und Host-Root-Anmeldeinformationen an ausgewählten Servern getestet. Führen Sie einen der folgenden Schritte aus:

   - Klicken Sie auf **Auswahl testen**. Die anderen Optionen sind inaktiv.
   - Klicken Sie auf **Alle Tests abbrechen**, um die Tests abzubrechen.
10. Klicken Sie auf **Speichern**, um das Profil abzuschließen.
11. Klicken Sie auf **Speichern und fortfahren**, um mit der Konfiguration von Ereignissen und Alarmen fortzufahren.

Konfigurieren von Ereignissen und Alarmen [Assistent]

Sie können Ereignisse und Alarme entweder mit dem Konfigurationsassistenten oder im Dell Management Center, Option „Einstellungen" für Ereignisse und Alarme konfigurieren.



ANMERKUNG: Auf Hosts vor der 12. Generation erfordert diese Funktion, dass das virtuelle Gerät als Trap-Ziel in OMSA konfiguriert wurde, um die Hostereignisse in vCenter anzuzeigen.

So konfigurieren Sie Ereignisse und Alarme:

1. Wählen Sie im **Konfigurationsassistenten** unter **Übermittlungsebene für das Ereignis** eine der folgenden Optionen:
   - Keine Ereignisse übermitteln – Hardware-Ereignisse blockieren.
   - Alle Ereignisse übermitteln – Alle Hardware-Ereignisse übermitteln.
   - Nur kritische Ereignisse und Warnungsereignisse übermitteln – Nur kritische und Warnungsereignisse der Hardware übermitteln.
   - Nur kritische Ereignisse und Warnungsereignisse hinsichtlich der Visualisierung übermitteln – Nur kritische und Warnungsereignisse im Zusammenhang mit der Virtualisierung übermitteln. Dies ist die Standardeinstellung für die Übermittlung von Ereignissen.
2. Aktivieren Sie das Kontrollkästchen **Alarme für Dell-Hosts aktivieren**, um alle Hardware-Alarme und -ereignisse zu aktivieren.

   ANMERKUNG: Dell-Hosts, auf denen Alarme aktiviert sind, reagieren auf kritische Ereignisse, indem sie in den Wartungsmodus übergehen.
3. Klicken Sie in dem Dialogfeld auf **Fortfahren**, um diese Änderung zu akzeptieren, oder klicken Sie auf **Abbrechen**.

   ANMERKUNG: Dieser Schritt wird nur dann angezeigt, wenn **Alarme für Dell Hosts aktivieren** ausgewählt wurde.
4. Klicken Sie auf **Standard Alarme wiederherstellen**, um die standardmäßigen Alarm-Einstellungen für alle Dell-Server im vCenter wiederherzustellen.

   Es kann bis zu einer Minute dauern, bis die Änderung übernommen wird.
5. Klicken Sie auf **Speichern und fortfahren**, um mit der Konfiguration im Assistenten fortzufahren.

Durch Wiederherstellen der OpenManage Integration for VMware vCenter-Gerätesicherung werden nicht alle Alarmeinstellungen wiederhergestellt. In der OpenManage-Integration for VMware-GUI werden die wiederhergestellten Einstellungen jedoch im Feld **Ereignisse und Alarme** angezeigt. Um dieses Problem zu beheben, ändern Sie die Einstellungen für Ereignisse und Alarme manuell auf der Registerkarte **Einstellungen** → **verwalten** in der OpenManage Integration for VMware-GUI.



ANMERKUNG: Nach dem Wiederherstellen des Geräts werden die Einstellungen für die Ereignisse und Alarme nicht aktiviert, selbst wenn sie die grafische Benutzeroberfläche als aktiviert anzeigt. Sie müssen die Einstellungen für die Ereignisse und Alarme auf der Seite „Einstellungen" erneut aktivieren

Einrichten eines Proxyservers [Assistent]

Das Einrichten des Proxyservers kann sofort im Konfigurationsassistenten oder später über die Seite **Einstellungen** → **Proxy** im Dell Management Center erfolgen.
So richten Sie einen Proxyserver ein:

1. Führen Sie im Fenster **HTTP-Proxy konfigurieren** einen der folgenden Schritte aus:
   - Klicken Sie auf **Speichern und fortfahren**, wenn Sie keinen Proxyserver verwenden.

- Wenn Sie einen Proxyserver verwenden, geben Sie unter **Einstellungen** eine **Proxyserver-Adresse** ein.

2. Geben Sie die **Proxy-Schnittstellennummer** ein.
3. Aktivieren Sie, falls erforderlich, das Kontrollkästchen **Anmeldeinformationen erforderlich**.
4. Wenn Sie das Kontrollkästchen **Anmeldeinformationen erforderlich** aktiviert haben, führen Sie Folgendes aus:
   a. Geben Sie den Proxy-Benutzernamen in das Textfeld **Proxy-Benutzername** ein.
   b. Geben Sie das Proxy-Kennwort in das Textfeld **Proxy-Kennwort** ein.
   c. Geben Sie das Proxy-Kennwort in das Textfeld **Kennwort überprüfen** erneut ein.
5. Aktivieren Sie unter **Proxy** das Kontrollkästchen **Proxy verwenden**.
6. Klicken Sie auf **Speichern und fortsetzen**, um die Änderungen zu übernehmen und fortzusetzen.

Planen von Jobs zum Erstellen von Bestandsaufnahmen [Assistent]

Die Vorgehensweise bei der Konfiguration eines Zeitplans zum Erstellen einer Bestandsaufnahme ähnelt der im Konfigurationsassistenten und den Optionen **Einstellungen** → **Dell Management Center**. Der wesentliche Unterschied besteht darin, dass der Assistent eine Option bietet, über die Sie die Bestandsaufnahme sofort erstellen können.



ANMERKUNG: Um sicherzustellen, dass die OpenManage Integration for VMware vCenter weiterhin aktualisierte Informationen anzeigt, wird empfohlen, dass Sie einen regelmäßigen Bestandsaufnahme-Job planen. Der Bestandsaufnahme-Job erfordert nur minimale Ressourcen und wirkt sich nicht negativ auf die Hostleistung aus.

So planen Sie einen Bestandsaufnahme-Job:

1. Führen Sie im **Konfigurationsassistent** im Fenster **Zeitplan Bestandsaufnahme** einen der folgenden Schritte aus:
   - Klicken Sie zum Ausführen von Zeitplänen zum Erstellen von Bestandsaufnahmen auf **An ausgewählten Tagen**.
   - Wählen Sie **Führen Sie keine Bestandsaufnahme auf Dell Hosts aus**, um Zeitpläne zum Erstellen von Bestandsaufnahmen nicht auszuführen.
2. Wenn Sie die Option **An ausgewählten Tagen** wählen, führen Sie Folgendes aus:
   a. Aktivieren Sie die Kontrollkästchen neben den Wochentagen, an denen eine Bestandsaufnahme erstellt werden soll.
   b. Geben Sie die Uhrzeit in dem Format HH:MM in das Textfeld ein.

      Die Zeit, die Sie eingeben, ist Ihre lokale Zeit. Wenn Sie daher beabsichtigen, die Bestandsaufnahme in der Zeitzone des virtuellen Geräts auszuführen, berechnen Sie den Zeitunterschied zwischen Ihrer Lokalzeit und der Zeitzone des virtuellen Geräts und geben dann die Zeit entsprechend ein.
3. Klicken Sie auf **Speichern und fortfahren**, um die Änderungen zu übernehmen und fortzufahren.

Ausführen eines Garantieabfrage-Jobs [Assistent]

Die Konfiguration des Garantieabruf-Jobs ist im Assistenten und in der Option **Einstellungen** → **Dell Management Centers** einander ähnlich. Darüber hinaus können Sie den Garantieabruf-Job von derJob-Warteschlange aus sofort ausführen.

So führen Sie einen Garantieabfrage-Job aus:

1. Führen Sie im **Konfigurationsassistenten** im Fenster **Garantiezeitplan** einen der folgenden Schritte aus:
   - Klicken Sie zum Ausführen von Garantiezeitplänen auf **An ausgewählten Tagen**.
   - Um Garantiezeitpläne nicht auszuführen, wählen Sie **Garantiedaten nicht abfragen** aus.
2. Wenn Sie die Option **An ausgewählten Tagen** wählen, führen Sie Folgendes aus:
   a. Aktivieren Sie das Kontrollkästchen neben jedem Wochentag, an dem die Garantieabfrage-Jobs ausgeführt werden sollen.
   b. Geben Sie die Uhrzeit in dem Format HH:MM in das Textfeld ein.

Die von Ihnen eingegebene Zeit ist Ihre Zeit vor Ort. Wenn Sie beabsichtigen, die Bestandsaufnahme zu der Zeit des virtuellen Geräts durchzuführen, berechnen Sie den Zeitunterschied zwischen der Zeitzone Ihres lokalen und virtuellen Geräts und geben Sie dann die Zeit entsprechend ein.

3. Klicken Sie auf **Speichern und fortfahren**, um die Änderungen zu übernehmen und fortzufahren.

Konfigurieren des Anmeldeinformationen für die Bereitstellung [Assistent]

Die Anmeldeinformationen für die Bereitstellung werden für die sichere Kommunikation mit einem Bare-Metal-System verwendet wird, das mit Hilfe der Auto-Erkennung erkannt wird. Für eine sichere Kommunikation wird iDRAC von der ersten Erfassung bis zum Ende des Bereitstellungsprozesses verwendet. Nach Abschluss der Bereitstellung werden die Anmeldeinformationen in die Informationen im Verbindungsprofil geändert, das dem Bare-Metal-System vom Bereitstellungsassistenten zugewiesen wurde. Wenn die Anmeldeinformationen für die Bereitstellung geändert werden, werden allen neu erfassten Systemen von diesem Zeitpunkt mit den neuen Anmeldeinformationen bereitgestellt. Beachten Sie jedoch, dass die Anmeldeinformationen auf den Servern, die vor der Änderung erfasst wurden, davon nicht betroffen sind.



ANMERKUNG: OpenManage Integration for VMware vCenter dient als Bereitstellungsserver. Die Anmeldeinformationen für die Bereitstellung werden auf dem iDRAC festgelegt, der das Plug-in als Bereitstellungsserver während der automatischen Ermittlung verwendet.

So konfigurieren Sie die Anmeldeinformationen für die Bereitstellung:

1. Sie können die Anmeldeinformationen im Fenster **Anmeldeinformationen für die Bereitstellung** anzeigen oder ändern. Der Bare-Metal-Server wechselt von diesen Anmeldeinformationen auf die im Verbindungsprofil.
2. Führen Sie zum Ändern dieser Anmeldeinformationen die folgenden Schritte unter **Anmeldeinformationen für die Bereitstellung eines Bare-Metal-Servers** aus:
   a. Im Textfeld **Benutzername** können Sie den Benutzernamen ändern.
   b. Im Textfeld **Kennwort** können Sie das Kennwort ändern.
   c. Geben Sie das Kennwort zur Bestätigung in das Textfeld **Kennwort bestätigen** ein.
3. Klicken Sie zum Speichern der angegebenen Anmeldeinformationen und zum Fortfahren des Konfigurationsassistenten auf **Speichern und fortfahren**.

Einrichten eines Standardeinstellung für die Repository der Firmware-Aktualisierungen [Assistent]

Einstellungen für das Firmware-Repository enthalten den Speicherort des Firmware-Katalogs, der zum Aktualisieren von bereitgestellten Servern verwendet wird. Sie können das Firmware-Repository entweder hier im Assistenten oder später mit der Option**Dell Management Center → Einstellungen** einrichten. Darüber hinaus können Sie die Firmware-Aktualisierung später von der Registerkarte „OpenManage Integration" ausführen.

So richten Sie die Standardeinstellung für die Repository der Firmware-Aktualisierung ein:

1. Wählen Sie im **Konfigurationsassistenten** auf der Seite **Firmware-Repository** das Standard-Repository für Firmware-Aktualisierungen aus, in dem Sie auf eine der folgenden Optionen klicken:

   - Dell Online

     Standard-Firmware-Repository (ftp.dell.com) mit einem Stagingordner. Das OpenManage Integration for VMware vCenter lädt die ausgewählten Firmware-Aktualisierungen herunter und speichert sie im Stagingordner. Dann werden sie nach Bedarf angewendet.
   - Lokales/freigegebenes Repository

Sie werden mit der Dell Repository Manager-Anwendung erstellt. Diese lokalen Repositories sollten sich in Windows-basierten Dateifreigaben befinden.

2. Wenn Sie die Option **Lokales/freigegebenes Repository** auswählen, führen Sie Folgendes aus:
   a. Geben Sie den **Speicherort der Katalogdatei** in der folgenden Syntax ein:
      - NFS-Freigabe für xml-Datei: host:/share/filename.xml
      - NFS-Freigabe für gz-Datei: host: /share/filename.gz
      - CIFS-Freigabe für xml-Datei: \\host\share/filename.xml
      - CIFS-Freigabe für gz-Datei: \\host\share/filename.gz
   b. Wenn Sie eine CIFS-Freigabe verwenden, geben Sie Werte in die Felder **Benutzername, Kennwort** und **Kennwort bestätigen** ein, die Kennwörter müssen gleich sein. Diese Felder sind nur dann aktiv, wenn Sie eine CIFS-Freigabe verwenden.

      ANMERKUNG: Das Zeichen „@“ wird für die Verwendung in Benutzernamen/Kennwörtern für freigegebene Netzwerkordner nicht unterstützt,
   c. Klicken Sie zum Überprüfen Ihrer Einträge auf **Test starten**.
3. Klicken Sie zum Speichern dieser Auswahl und zum Fortfahren des **Konfigurationsassistenten** auf **Speichern und Fortfahren**.

Aktivieren des OMSA-Links [Assistent]

Als Voraussetzung zum Starten von OMSA (OpenManage Server Administator) innerhalb des virtuellen Geräts der OpenManage Integration for VMware vCenter muss der OMSA-Webserver installiert und konfiguriert sein. Anweisungen, wie Sie den Webserver installieren und konfigurieren finden Sie im *Dell OpenManage Server Administrator Installation Guide* (Dell OpenManage Server Administrator-Installationshandbuch).

 **ANMERKUNG:** OMSA ist nur auf Dell-Servern vor Dell PowerEdge-Servern der 12. Generation erforderlich.

Sie können OMSA für folgende Zwecke verwenden:

- Verwalten von vCenter-Elementen (detaillierte Informationen zum Sensor/Komponenten-Status).
- Löschen von Befehlsprotokollen und Systemereignisprotokollen (SELs).
- Ermitteln von NIC-Statistiken.
- Stellen Sie sicher, dass OpenManage Integration for VMware vCenter die Ereignisse eines ausgewählten Hosts erfasst.

1. Geben Sie im **Konfigurationsassistenten** auf der Seite **OpenManage Server Admin** die OMSA-URL in das Textfeld **OMSA Webserver-URL** ein. Sie müssen die vollständige Internetadresse mit HTTPS und der Port-Nummer eingeben. Zum Beispiel,

   https:\\<OMSA_Server_IP_or_hostname>:1311.
2. Klicken Sie zum Speichern dieser URL und zum Beenden des Konfigurationsassistenten auf **Fertigstellen**.

Konfigurieren von NFS-Freigaben

Zum Verwenden von NFS-Freigaben mit dem OpenManage Integration for VMware vCenter für Backups und Wiederherstellung, Firmware-Aktualisierungen und als Sicherheitsverzeichnis müssen bestimmte Elemente konfiguriert werden. CIFS-Freigaben erfordern keine zusätzliche Konfiguration.

So konfigurieren Sie NFS-Freigaben:

1. Fügen Sie auf der Linux- oder Unix OS-Maschine, auf der die NFS-Freigaben gehostet werden, bei **/etc/exports** Folgendes hinzu: **/share/path <Geräte-IP> (rw) *(ro)**.

So hat das virtuelle Gerät vollständigen Schreib- und Lesezugriff auf die Freigabe, alle anderen Benutzer sind jedoch auf den Lesezugriff beschränkt.

2. Starten Sie die nfs-Services:

```
service portmap start service nfs start service nfslock status
```

ANMERKUNG: Die oben aufgeführten Schritte hängen von der verwendeten Linux-Distribution ab.

3. Falls bereits Services ausgeführt werden:

```
exportfs -ra
```

Einstellungen – Übersicht

Sie können die folgenden Aufgaben vom Abschnitt „Einstellungen“ her ausführen:

- Allgemein: Legt die OMSA URL fest, die auf der Registerkarte „Dell Hosts“ im vCenter angezeigt wird. Sie können auch „Warranty Expiration Notification“ (Benachrichtigung bei Ablauf der Garantie) aktivieren oder deaktivieren.
- Ereignisse und Alarme: Aktiviert oder deaktiviert alle Hardware-Alarme (der aktuelle Alarmstatus wird auf der Registerkarte „Alarme“ angezeigt). Konfiguriert darüber hinaus eingehende Ereignisse und die Warnungsfilterung.
- HTTP-Proxy: Aktiviert oder deaktiviert die Nutzung des HTTP-Proxyservers bei der Kommunikation mit Sites im Internet.
- Zeitplan Bestandsaufnahme: Legt einen Zeitplan für eine vCenter Host-Bestandsaufnahme fest.
- Garantiezeitplan: Legt einen Zeitplan für das Abrufen von Garantieinformationen für Dell-Hosts von Dell Online fest.
- Anmeldeinformationen für die Bereitstellung: Legt die Anmeldeinformationen fest, die während der ersten Erfassung und der Bereitstellung der Bare-Metal-Server für die Kommunikation mit Dell-Servern verwendet werden.
- Firmware-Repository: Hier liegen Sie fest, wo die Firmware-Aktualisierungen gespeichert werden.
- Sicherheit: Stellt eine Server-Weiße Liste bereit, die die bereits bereitgestellten Server beschränkt.

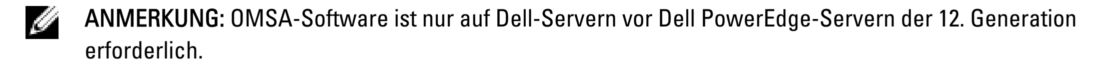
Allgemeine Einstellungen – Übersicht

Allgemeine Einstellungen dienen zum:

- Definieren der Internetadresse von OpenManage Server Administrator (OMSA).
- Aktivieren oder Deaktivieren der Benachrichtigung bei Ablauf der Garantie.

Die OMSA-Software kann für Folgendes verwendet werden:

- Verwalten von vCenter-Elementen (detaillierte Informationen zum Sensor/Komponenten-Status).
- Löschen von Befehlsprotokollen und Systemereignisprotokollen (SELs).
- Ermitteln von NIC-Statistiken.
- Stellen Sie sicher, dass OpenManage Integration for VMware vCenter die Ereignisse eines ausgewählten Hosts erfasst.



ANMERKUNG: OMSA-Software ist nur auf Dell-Servern vor Dell PowerEdge-Servern der 12. Generation erforderlich.

Die Benachrichtigung bei Ablauf der Garantie kann für Folgendes verwendet werden:

- Überwachen des Garantie-Ablaufdatums.
- Einstellen eine Mindestanzahl an Garantietagen, unter der entweder eine Warnung oder ein kritischer Alarm ausgelöst wird. Der Alarm erscheint als ein Symbol auf der Registerkarte „OpenManage Integration“ des Hosts.

Verwandte Aufgaben:

- Aktivieren des OMSA-Links
- Aktivieren oder Deaktivieren der Benachrichtigung bei Ablauf der Garantie

Aktivieren des OMSA-Links außerhalb des Konfigurationsassistenten

Als Voraussetzung zum Starten von OpenManage Server Administrator (OMSA) innerhalb des virtuellen Geräts des OpenManage Integration for VMware vCenter muss der OMSA-Webserver installiert und konfiguriert sein. Anweisungen, wie Sie den Webserver für die verwendete OMSA-Version installieren und konfigurieren, finden Sie im *Dell OpenManage Server Administrator Installation Guide* (Installationshandbuch für Dell OpenManage Server Administrator).

 **ANMERKUNG:** OMSA ist nur auf Dell-Servern vor Dell PowerEdge-Servern der 12. Generation erforderlich.

So aktivieren Sie den OMSA-Link:

1. Klicken Sie im **Dell Management Center Einstellungen** → **Allgemeines** unter „OMSA-Startprogramm“ auf **Bearbeiten**.
2. Geben Sie die Internetadresse für OSMA in das Textfeld **OMSA Web Server URL** ein. Sie müssen die vollständige Internetadresse einschließlich HTTPS und die Schnittstellennummer 1311 eingeben.
3. Klicken Sie zum Speichern dieser URL auf **Anwenden.**

   Weitere Informationen zum Einrichten eines OMSA-Trap-Ziels finden Sie unter Einrichten eines OMSA-Trap-Ziels.

Aktivieren oder Deaktivieren der Benachrichtigung bei Ablauf der Servergarantie

Die Garantieeinstellungen legen fest, wann Servergarantieinformationen von Dell online abgerufen werden. Dazu aktivieren oder deaktivieren Sie den Garantieplan und legen einen Schwellenwert für den Alarm „Minimum (Tage)“ fest. Auf dieser Seite können Sie Benachrichtigungen bei Ablauf der Servergarantie für Hosts und Cluster aktivieren oder deaktivieren. Diese Funktion wird im Dell Management Center unter „Einstellungen“, Seite „Allgemeines“ eingerichtet oder bearbeitet.

So aktivieren oder deaktivieren Sie Benachrichtigungen bei Ablauf der Servergarantie:

1. Klicken Sie im **Dell Management Center** auf **Einstellungen** → **Allgemeines**.
2. Aktivieren Sie auf der Seite **Allgemeines** das Kontrollkästchen **Benachrichtigungen über Garantiestatus aktivieren**, um Benachrichtigungen zu erhalten.
3. Führen Sie zum Festlegen des Alarms **Minimum (Tage) für Schwellenwertwarnung** die folgenden Schritte aus:
   a. Wählen Sie die Anzahl an Tagen für Warnungen über den Status der Servergarantie in der Dropdown-Liste **Warnungen** aus.
   b. Wählen Sie die Anzahl an Tagen für Warnungen über einen kritischen Status der Servergarantie in der Dropdown-Liste **Kritisch** aus.
4. Klicken Sie auf **Anwenden**, um die Änderungen zu übernehmen.

Erstellen eines neuen Verbindungsprofils

Ein Verbindungsprofil speichert die Anmeldeinformationen, die das virtuelle Gerät für die Kommunikation mit Dell Servern verwendet. Jeder Dell Server darf nur einem Verbindungsprofil zugeordnet sein, damit er vom OpenManage Integration for VMware vCenterverwaltet werden kann. Sie können mehrere Server zu einem Verbindungsprofil zuweisen. Das Verfahren zum Erstellen des Verbindungsprofils ist im Konfigurationsassistenten und im **Dell Management Center** → **Einstellungen** nahezu identisch. Sie können den Konfigurationsassistenten ausführen, wenn Sie das erste Mal auf die Dell Management-Konsole zugreifen, oder ihn später über das Fenster „Einstellungen“ aufrufen.

 **ANMERKUNG:** Mit Installationen auf Hosts der 12. Generation von Dell PowerEdge-Servern und später ist eine Installation des OMSA-Agenten nicht erforderlich. Bei Installationen auf Dell PowerEdge-Servern der 11. Generation wird der OMSA-Agent nun automatisch während des Bereitstellungsprozesses installiert.

ANMERKUNG: Beziehen Sie sich auf Informationen über OpenManage Integration for VMware vCenter-Lizenzierung für weitere Informationen über Lizenzierung.

ANMERKUNG: Sie können ein Verbindungsprofil nicht erstellen, falls die Anzahl an hinzugefügenen Hosts das Lizenzlimit überschreitet.

So erstellen Sie ein neues Verbindungsprofil:

1. Klicken Sie im linken Fensterbereich der **OpenManage Integration for VMware vCenter** auf **Verbindungsprofile**.
2. Geben Sie auf der Seite **Profilname und Beschreibung** den **Namen des Verbindungsprofils** und eine optionale **Beschreibung des Verbindungsprofils** ein, die dabei helfen, benutzerdefinierte Verbindungsprofile zu verwalten.
3. Wählen Sie auf der Seite **Zugewiesene Hosts** die Hosts für das Verbindungsprofil aus und klicken Sie auf **Weiter**.
4. Lesen Sie die Informationen auf der Seite **Anmeldeinformationen** und klicken Sie auf **Weiter**.
5. Auf der iDRAC-Seite, unter Anmeldeinformationen, führen Sie eine der folgenden Optionen aus:

   ANMERKUNG: Das iDRAC-Konto erfordert Administratorberechtigungen für die Aktualisierung der Firmware, Anwendung von Hardware-Profilen und die Bereitstellung des Hypervisors.

   - Für iDRACs, die für Active Directory, auf dem Sie Active Directory benutzen möchten, bereits konfiguriert und aktiviert sind, wählen Sie das Kontrollkästchen **Active Directory verwenden** aus; anderenfalls gehen Sie nach unten, um die iDRAC-Anmeldeinformationen zu konfigurieren.
     – Geben Sie im Textkästchen **Active Directory-Benutzername** den Benutzernamen ein. Geben Sie den Benutzernamen in einem dieser Formate ein: Domain\Benutzername oder Domain/Benutzername oder username@domain. Der Benutzername darf maximal 256 Zeichen enthalten. Weitere Informationen zu Benutzernamen-Einschränkungen finden Sie in der Dokumentation zu Microsoft Active Directory.
     – Geben Sie im Textfeld **Active Directory-Kennwort** das Kennwort ein. Das Kennwort darf maximal 127 Zeichen enthalten.
     – Geben Sie das Kennwort zur Bestätigung in das Textfeld **Kennwort bestätigen** ein.
     – Wählen Sie in der Zertifikatsprüfung-Drop-Down-Liste eine der folgenden Optionen aus:
       * Wählen Sie **Aktivieren** aus, um das iDRAC-Zertifikat herunterzuladen, zu speichern und für alle künftigen Verbindungen zu validieren.
       * Wählen Sie **Deaktivieren**, um keine Prüfung durchzuführen und das Zertifikat nicht zu speichern.
   - Um iDRAC-Anmeldeinformationen ohne Active Directory zu konfigurieren, führen Sie Folgendes aus:
     – Geben Sie im Textfeld **Benutzername** den Benutzernamen ein. Der Benutzername darf maximal 16 Zeichen enthalten. Weitere Informationen zur Benutzername-Einschränkungen für Ihre Version von iDRAC finden Sie in der iDRAC-Dokumentation.

       ANMERKUNG: Das lokale iDRAC-Konto erfordert Administratorberechtigungen für die Aktualisierung der Firmware, Anwendung von Hardware-Profilen und die Bereitstellung des Hypervisors.
     – Geben Sie im Textfeld **Kennwort** das Kennwort ein. Das Kennwort darf maximal 20 Zeichen enthalten.
     – Geben Sie das Kennwort zur Bestätigung in das Textfeld **Kennwort bestätigen** ein.
     – Wählen Sie in der Zertifikatsprüfung-Drop-Down-Liste eine der folgenden Optionen aus:
       * Wählen Sie **Aktivieren** aus, um das iDRAC-Zertifikat herunterzuladen, zu speichern und für alle künftigen Verbindungen zu validieren.
       * Wählen Sie **Deaktivieren**, um keine Prüfung durchzuführen und das iDRAC-Zertifikat nicht zu speichern.
6. Klicken Sie auf **Weiter**.

7. Auf der iDRAC-Seite, unter Host-Anmeldeinformationen, führen Sie eine der folgenden Optionen aus:

   - Für Hosts, die für Active Directory, auf dem Sie Active Directory benutzen möchten, bereits konfiguriert und aktiviert sind, wählen Sie das Kontrollkästchen **Active Directory verwenden** aus; anderenfalls gehen Sie nach unten, um Ihre Host-Anmeldeinformationen zu konfigurieren.

     – Geben Sie im Textkästchen **Active Directory-Benutzername** den Benutzernamen ein. Geben Sie den Benutzernamen in einem dieser Formate ein: Domain\Benutzername oder Domain/Benutzername oder username@domain. Der Benutzername darf maximal 256 Zeichen enthalten. Weitere Informationen zu Benutzernamen-Einschränkungen finden Sie in der Dokumentation zu Microsoft Active Directory.
     – Geben Sie im Textfeld **Active Directory-Kennwort** das Kennwort ein. Das Kennwort darf maximal 127 Zeichen enthalten.
     – Geben Sie das Kennwort zur Bestätigung in das Textfeld **Kennwort bestätigen** ein.
     – Wählen Sie in der Zertifikatsprüfung-Drop-Down-Liste eine der folgenden Optionen aus:

       * Wählen Sie **Aktivieren** aus, um das Host-Zertifikat herunterzuladen, zu speichern und für alle künftigen Verbindungen zu validieren.
       * Wählen Sie **Deaktivieren**, um keine Prüfung durchzuführen und das Host-Zertifikat nicht zu speichern.

   - Um Host-Anmeldeinformationen ohne Active Directory zu konfigurieren, führen Sie Folgendes aus:

     – Geben Sie in das Feld **Benutzername** den Namen des Benutzers ein. Die schreibgeschützte Standardeinstellung für den Benutzernamen ist „root". Wenn Sie die Option **Active Directory verwenden** wählen, kann der Benutzername von „root" abweichen.
     – Geben Sie im Textfeld **Kennwort** das Kennwort ein. Das Kennwort darf maximal 127 Zeichen enthalten.

       ANMERKUNG: Die OMSA-Anmeldeinformationen sind die gleichen, die auch für ESX- und ESXi-Hosts verwendet werden.

     – Geben Sie das Kennwort zur Bestätigung in das Textfeld **Kennwort bestätigen** ein.
     – Wählen Sie in der Zertifikatsprüfung-Drop-Down-Liste eine der folgenden Optionen aus:

       * Wählen Sie **Aktivieren** aus, um das Host-Zertifikat herunterzuladen, zu speichern und für alle künftigen Verbindungen zu validieren.
       * Wählen Sie **Deaktivieren**, um keine Prüfung durchzuführen und das Host-Zertifikat nicht zu speichern.

8. Klicken Sie auf **Weiter**.
9. Der Link **Testverbindung** wird verwendet, um die bereitgestellten iDRAC-und Host-Anmeldeinformationen für die ausgewählten Server zu überprüfen. Führen Sie einen der folgenden Schritte aus:

   - Klicken Sie auf **Auswahl testen**. Die anderen Optionen sind inaktiv.
   - Klicken Sie auf **Tests abbrechen**, um die Tests abzubrechen.

   ANMERKUNG: Bei Servern, die nicht über eine iDRAC Express- oder iDRAC Enterprise-Karte verfügen, lautet das Ergebnis für den iDRAC-Verbindungstest „Für dieses System nicht anwendbar“.

10. Klicken Sie auf **Speichern**, um das Profil abzuschließen.

    Weitere Informationen zum Verwalten von Verbindungsprofilen finden Sie unter Verwalten von Verbindungsprofilen.

Konfigurieren von Ereignissen und Alarmen

Auf der Seite „Ereignisse und Alarme“ im Dell Management Center werden alle Hardware-Alarme aktiviert oder deaktiviert. Der aktuelle Alarm-Status wird auf der Registerkarte „Alarme“ im vCenter angezeigt. Ein kritisches Ereignis deutet auf einen tatsächlichen oder bevorstehenden Datenverlust oder auf einen Systemausfall hin. Ein Warnereignis

bedarf nicht unbedingt sofortiger Aufmerksamkeit, deutet aber auf ein mögliches zukünftiges Problem hin. Ereignisse und Alarme können auch mit dem VMware Alarm Manager aktiviert werden. Ereignisse werden auf der Registerkarte „Tasks und Ereignisse" im vCenter in der Ansicht „Hosts und Cluster" angezeigt.



ANMERKUNG: Bei Hosts vor der Version der Dell PowerEdge-Server der 12. Generation erfordert diese Funktion, dass das virtuelle Gerät als ein Trap-Ziel in OMSA konfiguriert ist, um Host-Ereignisse im vCenter anzuzeigen. Weitere Informationen zu OMSA finden Sie unter Einrichten eines OMSA Trap-Zieles.

Sie können Ereignisse und Alarme auch im Dell Management Center unter der Option „Einstellungen" für Ereignisse und Alarme einrichten.
So konfigurieren Sie Ereignisse und Alarme:

1. Klicken Sie im **Dell Management Center** unter **Einstellungen** → **Ereignisse und Alarme** auf **Bearbeiten.**
2. Wählen Sie eine der folgenden Optionen unter **Übermittlungsebene für das Ereignis**:
   - Keine Ereignisse übermitteln – Hardware-Ereignisse blockieren.
   - Alle Ereignisse übermitteln – Alle Hardware-Ereignisse übermitteln.
   - Nur kritische Ereignisse und Warnungsereignisse übermitteln – Nur kritische und Warnungsereignisse der Hardware übermitteln.
   - Nur kritische Ereignisse und Warnungsereignisse hinsichtlich der Visualisierung übermitteln – Nur kritische und Warnungsereignisse im Zusammenhang mit der Virtualisierung übermitteln. Dies ist die Standardeinstellung für die Übermittlung von Ereignissen.
3. Aktivieren Sie das Kontrollkästchen **Alarme für Dell-Hosts aktivieren**, um alle Hardware-Alarme und -ereignisse zu aktivieren.

   ANMERKUNG: Dell-Hosts, auf denen Alarme aktiviert sind, reagieren auf kritische Ereignisse, indem sie in den Wartungsmodus übergehen.
4. Klicken Sie in dem Dialogfeld auf **Fortfahren**, um diese Änderung zu akzeptieren, oder klicken Sie auf **Abbrechen**.
5. Klicken Sie auf **Standard Alarme wiederherstellen**, um die standardmäßigen Alarm-Einstellungen für alle Dell-Server im vCenter wiederherzustellen.

   Es kann bis zu einer Minute dauern, bis die Änderung übernommen wird.
6. Klicken Sie zum Speichern auf **Speichern**.

Allgemeines zur Proxy-Konfiguration

Die Proxy-Einstellungen definieren den HTTP-Proxy sowie den erforderlichen Berechtigungsnachweis, der zum Abrufen von Informationen aus dem Web (auch von der Dell Online) erforderlich ist. Dazu gehören:

- Aktivieren oder Deaktivieren des Proxyservers
- Eingeben des Proxyservers und der erforderlichen Portnummer
- Definieren des erforderlichen Berechtigungsnachweis – Benutzername und Kennwort

Verwandte Aufgaben:

- Einrichten eines Proxyservers
- Verwenden des HTTP-Proxys zum Abrufen von Web-basierten Daten
- Einrichten des HTTP-Proxys mithilfe der Administrator-Konsole

Einrichten eines Proxyservers

Das Einrichten des Proxyservers kann sofort im Konfigurationsassistenten oder später über die Seite „Einstellungen > Proxy" im Dell Management Center erfolgen.



ANMERKUNG: Die Proxy-Kennwörter dürfen nicht mehr als 31 Zeichen umfassen.

So richten Sie einen Proxyserver ein:

1. Wählen Sie im Dell Management Center **Einstellungen** → **HTTP-Proxy** aus und klicken Sie auf **Bearbeiten**.
2. Führen Sie im Fenster **HTTP-Proxy** einen der folgenden Schritte aus:
    - Klicken Sie auf **Speichern und fortfahren**, wenn Sie keinen Proxyserver verwenden.
    - Wenn Sie einen Proxyserver verwenden, geben Sie unter **Einstellungen** eine **Proxyserver-Adresse** ein.
3. Geben Sie die **Proxy-Schnittstellennummer** ein.
4. Aktivieren Sie, falls erforderlich, das Kontrollkästchen **Anmeldeinformationen erforderlich**.
5. Wenn Sie das Kontrollkästchen **Anmeldeinformationen erforderlich** aktiviert haben, führen Sie Folgendes aus:
    a. Geben Sie den Proxy-Benutzernamen in das Textfeld **Proxy-Benutzername** ein.
    b. Geben Sie das Proxy-Kennwort in das Textfeld **Proxy-Kennwort** ein.
    c. Geben Sie das Proxy-Kennwort zur Bestätigung in das Textfeld **Kennwort bestätigen** ein.
6. Aktivieren Sie unter **Proxy** das Kontrollkästchen **Proxy verwenden**.
7. Klicken Sie zum Speichern dieser Optionen auf **Speichern**.

Verwenden des HTTP-Proxys zum Abrufen von Web-basierten Daten

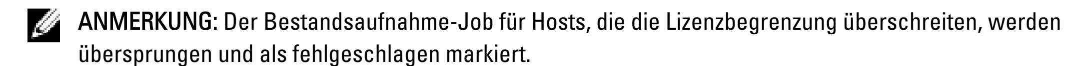
So verwenden Sie den HTTP-Proxy zum Abrufen von Web-basierten Daten:

1. Wählen Sie im **Dell Management Center Einstellungen** → **HTTP-Proxy** aus und klicken Sie auf **Bearbeiten**.
2. Aktivieren Sie das Kontrollkästchen **Proxy verwenden**.
3. Klicken Sie auf **Anwenden**.
4. Klicken Sie auf **Konnektivität testen**, um die Einstellungen zu überprüfen.

Ausführen von Bestandsaufnahme-Jobs

So führen Sie den Bestandsaufnahme-Job aus:

1. Nachdem der **Konfigurationsassistent** beendet wurde, klicken Sie auf **Job-Warteschlange** → **Bestandsaufnahme** → **Jetzt ausführen**, um sofort eine Bestandsaufnahme zu erstellen.
2. Klicken Sie auf **Aktualisieren**, um den Status des Bestandsaufnahme-Jobs zu aktualisieren.
3. Navigieren Sie zur Ansicht **Hosts und Cluster**, klicken Sie auf einen **Dell Host** und dann auf die Registerkarte **OpenManage Integration**. Die folgenden Informationen sollten angezeigt werden:
    - Übersicht
    - System-Ereignisprotokoll
    - Hardware-Bestandsaufnahme
    - Bei Lagerung
    - Firmware
    - Stromüberwachung
    - Garantiestatus

    ANMERKUNG: Der Bestandsaufnahme-Job für Hosts, die die Lizenzbegrenzung überschreiten, werden übersprungen und als fehlgeschlagen markiert.

    Die folgenden Host-Befehle funktionieren innerhalb der Registerkarte „OpenManage Integration“:

    - Blinkanzeigelicht
    - Firmware-Aktualisierungsassistent ausführen
    - Remote-Zugriff starten
    - OMSA starten

- CMC starten

Ausführen eines Garantieabfrage-Jobs

Die Konfiguration des Garantieabruf-Jobs mittels des Assistenten und über die Option **Dell Management Center → Einstellungen** ist ähnlich. Nach Ausführen des Assistenten können Sie ihn jederzeit von der Seite **Dell Management Center → Einstellungen → Garantiezeitplan** aus bearbeiten. Sie können den Garantieabruf-Job jetzt von der Seite **Job-Warteschlange → Garantieverlauf**aus ausführen.

So planen Sie einen Garantieabfrage-Jobs:

1. Wählen Sie im **Dell Management Center Einstellungen → Garantiezeitplan** aus.
2. Klicken Sie im Fenster **Garantiezeitplan** auf **Bearbeiten**.
3. Führen Sie zum Konfigurieren des Zeitplans die folgenden Schritte aus:
   a. Klicken Sie zum Ausführen von Garantiezeitplänen auf **An ausgewählten Tagen**.
   b. Wenn keine Garantiepläne ausgeführt werden sollen, wählen Sie **Führen Sie keine Bestandsaufnahme auf Dell Hosts aus**.
4. Wenn Sie die Option **An ausgewählten Tagen** wählen, führen Sie Folgendes aus:
   a. Aktivieren Sie das Kontrollkästchen neben den Wochentagen, an denen ein Garantieabfrage-Auftrag ausgeführt werden soll.
   b. Geben Sie die Uhrzeit in dem Format HH:MM in das Textfeld ein.

      Bei der von Ihnen eingegebenen Zeit muss es sich um die bei Ihnen geltende Ortszeit handeln. Berechnen Sie den Zeitunterschied, wenn der Garantieabfrage-Job zu einer bestimmten Zeit ausgeführt werden soll.
5. Zum sofortigen Ausführen des Garantieabfrage-Jobs wechseln Sie zu **Job-Warteschlange → Garantieverlauf** und klicken dann auf **Jetzt ausführen**.

Anzeigen bzw. Bearbeiten der Anmeldeinformationen für die Bereitstellung

Im Dell Management Center können Sie die Anmeldeinformationen für die Bereitstellung bearbeiten. Die Anmeldeinformationen für die Bereitstellung werden für die sichere Kommunikation mit einem Bare-Metal-System verwendet; dabei wird iDRAC von der ersten Erfassung bis zum Ende des Bereitstellungsprozesses verwendet. Nach Abschluss der Bereitstellung werden die Anmeldeinformationen auf die Informationen im Verbindungsprofil geändert, das dem Bare-Metal-System vom Bereitstellungsassistenten zugewiesen wurde. Wenn die Anmeldeinformationen für die Bereitstellung geändert werden, werden allen neu erfassten Systemen von diesem Zeitpunkt an die neuen Anmeldeinformationen bereitgestellt. Dies betrifft jedoch nicht die Anmeldeinformationen auf den Servern, die vor der Änderung erfasst wurden. Der Benutzername darf nicht mehr als 16 (ASCII-druckbare Zeichen) umfassen. Das Kennwort darf nicht mehr als 20 (ASCII-druckbare Zeichen) umfassen.
So zeigen Sie die Anmeldeinformationen für die Bereitstellung an bzw. bearbeiten sie:

1. Klicken Sie im **Dell Management Center → Einstellungen → Anmeldeinformationen für Bereitstellung** und **Bearbeiten**.
2. Führen Sie in **Anmeldeinformationen für die Bereitstellung eines Bare-Metal-Servers** unter **Anmeldeinformationen** die folgenden Schritte aus:
   - Geben Sie den Benutzernamen in das Textfeld **Benutzername** ein.

     Der Benutzername darf nicht mehr als 16 (ASCII-druckbare Zeichen) umfassen.
   - Geben Sie das Kennwort in das Textfeld **Kennwort** ein.

     Das Kennwort darf nicht mehr als 20 (ASCII-druckbare Zeichen) umfassen.
   - Geben Sie das Kennwort zur Bestätigung in das Textfeld **Kennwort bestätigen** ein.

     Die Kennwörter müssen identisch sein.
3. Klicken Sie auf **Anwenden**.

Einrichten des Firmware-Repositorys

So richten Sie das Formular-Repository und den Berechtigungsnachweis ein:

1. Wählen Sie in der **OpenManage Integration for VMware vCenter Einstellungen** → **Firmware-Repository**aus und klicken Sie dann auf **Bearbeiten**.
2. Wählen Sie im **Firmware-Repository** das Standard-Repository für Firmware-Aktualisierungen aus, in dem Sie auf eine der folgenden Optionen klicken:
    - **Dell Online**
      Diese Funktion verwendet das Standard-Repository für Firmware-Aktualisierungen von Dell-Online (ftp.dell.com) mit einem erforderlichen Stagingordner. Die OpenManage Integration for VMware vCenterlädt die ausgewählten Firmware-Aktualisierungen herunter und speichert sie im Stagingordner. Dann werden sie nach Bedarf angewendet.
    - **Freigegebene Netzwerkordner**
      Hosts, die Lifecycle Controller verwenden, können von einem benutzerdefinierten Repository, das auf einem im Netzwerk freigegebenen Ordner gehostet ist, aktualisieren. Um ein benutzerdefiniertes Repository zu erstellen, empfiehlt Dell die Verwendung des Dell Repository Managers zum Erstellen and Speichern desselben an einem gemeinsam genutzten Speicherort, an dem die Hosts und OpenManage Integration darauf zugreifen kann. Geben Sie den Speicherort der Repository-Katalogdatei unten ein.
3. Wenn Sie **Freigegebenen Netzwerkordner** auswählen, geben Sie die Katalogdatei im Feld **Speicherort der Katalogdatei ein.**
4. Klicken Sie auf **Test starten**.
5. Klicken Sie auf **Anwenden**.

Server-Sicherheitseinstellungen für die Bereitstellung

Beschränken Sie die bereitstellungsfähigen Server mithilfe einer weißen Liste. Wenn sich ein Server in der weißen Liste befindet, wird er während der Auto-Discovery und des Handshakings mit Anmeldeinformationen versorgt und in der Liste der Server angezeigt, die für die Bereitstellung verwendet werden. Die weiße Liste wird durch manuelles Hinzufügen von Server-Service-Tags, Löschen von Service-Tags oder Importieren einer Liste von Service-Tags aus einer CSV-Datei verwaltet.



ANMERKUNG: Verwenden Sie eine CSV-Komma-getrennte-Datei zum Importieren von Servern. Diese Liste enthält zahlreiche Einträge in mehreren Zeilen, wobei jeder Eintrag einen oder mehrere durch Komma getrennte Service-Tags enthält.

Zum Einrichten und Verwalten von weißen Listen wählen Sie unter Folgendem:

- Aktivieren einer weißen Server-Liste
- Hinzufügen von Servern zu einer weißen Liste
- Löschen von Servern aus einer weißen Liste

Aktivieren einer weißen Liste bereitstellungsfähiger Server

Informationen zu den Sicherheitseinstellungen von bereitstellungsfähigen Servern finden Sie unter Server-Sicherheitseinstellungen für die Bereitstellung.

So aktivieren Sie eine Server-Weiße-Liste:

1. Wählen Sie im linken Fensterbereich im **Dell Management Center** die Option **Einstellungen**.
2. Wählen Sie im rechten Fensterbereich **Sicherheit** aus.

3. Klicken Sie im Fenster **Sicherheit** auf **Bearbeiten**.
4. Aktivieren Sie das Kontrollkästchen **Weiße Liste mit Servern durchsetzen**, um die Serverbereitstellung mithilfe der weißen Liste einzuschränken.
5. Klicken Sie auf **Anwenden**, die Einstellung für die Server-Weiße-Liste wird zu AKTIVIERT geändert.

Hinzufügen von bereitstellungsfähigen Servern zu einer weißen Liste

Informationen zu den Sicherheitseinstellungen von bereitstellungsfähigen Servern finden Sie unter Server-Sicherheitseinstellungen für die Bereitstellung. Es ist möglich, dass nur Dell-Server in der weißen Liste des Servers zur Bereitstellung mit dem OpenManage Integration for VMware vCenterzur Verfügung stehen. Sie können bereitstellungsfähige Server entweder manuell oder durch Importieren aus einer Liste zur einer weißen Liste hinzufügen.

So fügen Sie bereitstellungsfähige Server zu einer weißen Liste hinzu:

1. Wählen Sie im linken Fensterbereich im **Dell Management Center** die Option **Einstellungen** → **Sicherheit**.
2. Klicken Sie im Fenster **Weiße Liste mit Servern** auf **Bearbeiten** und führen Sie dann einen der folgenden Schritte aus:

   - Klicken Sie auf **Server hinzufügen**, um Server manuell zur weißen Liste hinzuzufügen.
     - Geben Sie die Service-Tag-Nummern in das Dialogfeld **Service-Tag-Nummern hinzufügen** ein.
     - Klicken Sie auf **Weiter**, um die Tags hinzuzufügen.
   - Klicken Sie auf **Weiße Liste importieren**, um eine Liste der Service-Tag-Nummern zu importieren.
     - Wenn das Dialogfeld **Hochzuladende Datei auswählen** angezeigt wird, suchen Sie die gewünschte csv-Datei aus und klicken auf **Öffnen**.

       Für ein Beispiel einer weißen Liste:

       ASDFG12

       SDCNRD0

       TESCVD3

       AS243AS, ASWERF3, FGVCSD9
     - Wenn das Dialogfeld **Wir haben diese Service-Tag-Nummern in Ihrer Datei gefunden** angezeigt wird, klicken Sie auf **Anwenden**.

   Die Service-Tag-Nummern werden jetzt in der Liste der Service-Tags angezeigt.

Löschen von bereitstellungsfähigen Servern aus einer weißen Liste

Informationen zu den Sicherheitseinstellungen von bereitstellungsfähigen Servern finden Sie unter Server-Sicherheitseinstellungen für die Bereitstellung.

So löschen Sie bereitstellungsfähige Server aus einer weißen Liste:

1. Wählen Sie im linken Fensterbereich im **Dell Management Center** die Option **Einstellungen**.
2. Wählen Sie im rechten Fensterbereich **Sicherheit** aus.
3. Klicken Sie im Fenster **Sicherheit** auf **Bearbeiten**.
4. Führen Sie einen der folgenden Vorgänge aus:

   - Aktivieren Sie das Kontrollkästchen **Service-Tag-Nummer**, um einen bestimmten Server zu löschen, und klicken Sie dann auf **Ausgewählte löschen**.
   - Aktivieren Sie das Kontrollkästchen **Service-Tag-Nummer**, um alle Server zu löschen, und klicken Sie dann auf **Ausgewählte löschen**.
5. Wenn das Dialogfeld **Sind Sie sicher, dass Sie die ausgewählten Service-Tag-Nummern löschen wollen?** angezeigt wird, klicken Sie auf **Anwenden** oder auf **Abbrechen**, um den Vorgang abzubrechen.

6. Klicken Sie auf **Anwenden**, um die Änderungen zu übernehmen.

Allgemeines zu Host-, Bare-Metal- und iDRAC-Konformitätsproblemen

Zum Verwalten von Hosts, Bare-Metal-Servern und iDRAC mit dem OpenManage Integration for VMware vCenter müssen bestimmte Mindestkriterien erfüllt sein. Wenn diese nicht erfüllt sind, können sie nicht ordnungsgemäß vom OpenManage Integration for VMware vCenter verwaltet werden. Verwenden Sie die Links „Einstellungen nicht konformer Hosts korrigieren", „Bare-Metal-Server" und „iDRAC-Konformität", um anzuzeigen, welche Hosts/Bare-Metal-Server/iDRACs in Ihrer Konfiguration nicht konform sind und korrigieren Sie die Einstellungen. Dieser Assistent zeigt Hosts/Bare-Metal-Server/iDRACs an, bei denen:

- Hosts keinem Verbindungsprofil zugeordnet wurden.

  Wenn kein Verbindungsprofil zu einem Host zugeordnet wurde, wird ein Dialogfeld angezeigt, über das Sie das Fenster „Verbindungsprofil" aufrufen können. Diese Konfiguration erfolgt dann außerhalb des Assistenten. Kehren Sie später zurück, um diesen Assistenten auszuführen.
- Das „Collect System Inventory on Reboot" (CSIOR) deaktiviert ist oder nicht ausgeführt wurde. Hierzu ist ein manueller Neustart erforderlich.
- Der OMSA-Agent (Host Root-Berechtigungsnachweis) nicht installiert wurde, veraltet ist oder nicht ordnungsgemäß konfiguriert wurde.
- Bare-Metal-Server veraltete Integrated Dell Remote Access Controller (iDRAC)-Firmware, Lifecycle Controller (LC)-Firmware oder BIOS-Versionen aufweisen.



VORSICHT: Hosts im Lockdown-Modus nicht in Konformitätsprüfungen angezeigt werden, auch wenn sie nicht konform sind. Sie werden nicht angezeigt, weil ihr Konformitätsstatus nicht ermittelt werden kann. Denken Sie daran, die Konformität dieser Systeme manuell zu prüfen, wenn eine Warnmeldung angezeigt wird.

In jedem Fall müssen Sie die Konformitätsprobleme beheben, indem Sie eine der folgenden Optionen ausführen:

- Zum Beheben von Konformitätsproblemen bei vSphere-Hosts lesen Sie Ausführen des Assistenten zum Beheben nicht konformer vSphere-Hosts
- Zum Beheben von Konformitätsproblemen bei Bare-Metal-Servern lesen Sie Ausführen des Assistenten zum Beheben nicht konformer Bare-Metal-Server
- Zum Beheben von Konformitätsproblemen bei iDRAC lesen Sie:iDRAC-Lizenzkonformität

Weitere Informationen:

- Erneute Prüfung der Bare-Metal-Server-Konformität
- Herunterladen eines ISO für manuelle Firmware-Aktualisierungen

Ausführen des Assistenten zum Beheben nicht konformer vSphere-Hosts

Führen Sie den Assistenten zum Beheben nicht konformer vSphere Hosts aus. Weitere Informationen zur Konformität finden Sie unter Allgemeines zu Host- und Bare-Metal-Konformitätsproblemen. Einige nicht konforme ESXi-Hosts müssen neu gestartet werden. Ein Neustart eines ESXi-Hosts ist erforderlich, wenn OpenManage Server Administrator (OMSA) installiert oder aktualisiert werden muss. Darüber hinaus ist ein Neustart für jeden Host erforderlich, der CSIOR noch nicht ausgeführt hat. Wenn Sie wählen, einen ESXi-Host automatisch neu zu starten, finden die folgenden Aktionen statt:

- Bei einer CSIOR-Statuskorrektur:

  Wenn die CSIOR-Funktion nicht auf dem Host aktiviert ist, wird der CSIOR auf dem Host auf *EIN* gestellt und anschließend in den Wartungsmodus versetzt und neu gestartet.

- Bei einer OMSA-Statuskorrektur:

  a. OMSA ist auf dem Host installiert.
  b. Der Host wird in den Wartungsmodus versetzt und neu gestartet.
  c. Nach dem Neustart ist OMSA so konfiguriert, dass alle Änderungen übernommen werden.
  d. Der Host beendet den Wartungsmodus.
  e. Eine Bestandsaufnahme wird erstellt, um die Daten zu aktualisieren.

So führen Sie den „Assistenten zum Beheben nicht konformer vSphere-Hosts“ aus:

1. Klicken Sie im linken Fensterbereich im **Dell Management Center** auf **Konformität** → **vSphere Hosts**.
2. Zeigen Sie im Fenster **Konformität der vSphere-Hosts** die nicht konformen Host an und klicken Sie dann auf **Nicht konforme vSphere-Hosts beheben**.
3. Aktivieren Sie im Assistenten **Nicht konforme vSphere-Hosts beheben** die Kontrollkästchen der Hosts, die Sie korrigieren möchten.
4. Klicken Sie auf **Weiter**.
5. Wenn ein Server ohne Verbindungsprofil vorhanden ist, haben Sie die Option, den Assistenten zu beenden und diese Systeme auf der Seite **Verbindungsprofil** zu korrigieren oder diesen Assistenten fortzusetzen. Lesen Sie dazu Erstellen eines neuen Verbindungsprofils. Nach Abschluss kehren Sie zu diesem Assistenten zurück.
6. Aktivieren Sie im Fenster **CSIOR aktivieren** die Kontrollkästchen, um **CSIOR** für die ausgewählten Hosts zu aktivieren.
7. Klicken Sie auf **Weiter**.
8. Aktivieren Sie im Fenster **OMSA beheben** die Kontrollkästchen, um **OMSA** für die ausgewählten Hosts zu korrigieren.
9. Klicken Sie auf **Weiter**.
10. Zeigen Sie im Fenster **Hosts neustarten** die ESXi-Hosts an, die neu gestartet werden müssen. Ein Neustart für einen ESXi-Host ist erforderlich, wenn OMSA installiert oder aktualisiert werden musste. Darüber hinaus ist ein Neustart für jeden Host erforderlich, auf dem CSIOR noch nicht ausgeführt wurde. Führen Sie einen der folgenden Schritte aus:

    - Wenn Sie Hosts bei Bedarf automatisch in den Wartungsmodus versetzen und neustarten möchten, aktivieren Sie das Kontrollkästchen **Hosts bei Bedarf automatisch in den Wartungsmodus versetzen und neustarten**.
    - Wenn Sie den Neustart manuell durchführen möchten, führen Sie die folgenden Schritte aus:

      1. Nachdem die Aufgabe *OMSA installieren* für einen Host abgeschlossen wurde, starten Sie den Host neu.
      2. Wenn der Host hochgefahren und OMSA nicht konfiguriert ist, konfigurieren Sie OMSA entweder manuell oder verwenden den Konformitätsassistenten.
      3. Erstellen Sie eine neue Bestandsaufnahme. Lesen Sie dazu Ausführen von Jobs zum Erstellen einer Bestandsaufnahme.
11. Klicken Sie auf **Weiter**.
12. Prüfen Sie die Maßnahmen, die an nicht konformen Hosts durchgeführt werden, im Fenster **Zusammenfassung**. Hierfür sind manuelle Neustarts erforderlich.
13. Klicken Sie auf **Fertigstellen**.

Ausführen des Assistenten zum Korrigieren der Einstellungen nicht konformer Bare-Metal-Server

Führen Sie den Assistenten zum Korrigieren der Einstellungen nicht konformer Bare-Metal-Server aus. Weitere Informationen zur Konformität finden Sie unter Allgemeines zu Host- und Bare-Metal-Konformitätsproblemen.

So führen Sie den Assistenten zum Korrigieren der Einstellungen nicht konformer Bare-Metal-Server aus:

1. Klicken Sie im linken Fensterbereich im **Dell Management Center** auf **Konformität** → **Bare-Metal-Server**.
2. Zeigen Sie die nicht konformen Hosts im Fenster **Bare-Metal-Server** an und klicken Sie dann auf **Nicht konforme Bare-Metal-Server beheben**.
3. Aktivieren Sie im Assistenten **Bare-Metal-Server beheben** die Kontrollkästchen der Hosts, die Sie korrigieren möchten.
4. Klicken Sie auf **Weiter**.
5. Prüfen Sie die Maßnahmen, die an nicht konformen Bare-Metal-Servern durchgeführt werden, im Fenster **Zusammenfassung**.
6. Klicken Sie auf **Fertigstellen**.

Erneute Prüfung der Bare-Metal-Server-Konformität

Bei Servern, die Sie außerhalb des OpenManage Integration for VMware vCenter repariert haben, müssen Sie diese Server-Konformitätsprüfung erneut manuell ausführen. Sie finden sie im Dell Management Center auf der Seite „Konformität > Bare-Metal-Server".

So prüfen Sie die Bare-Metal-Server-Konformität erneut:

1. Klicken Sie im **Dell Management Center** → **auf die Seite Konformität** → **Bare-Metal-Server** auf **Konformität erneut überprüfen**.
2. Klicken Sie zum Aktualisieren der Liste im Fenster **Nicht konforme Server** auf **Aktualisieren**.
3. Klicken Sie zum erneuten Prüfen auf **Konformität überprüfen**.
4. Klicken Sie zum Abbrechen der erneuten Prüfung auf **Alle Tests abbrechen**.
5. Nachdem Sie Ihr System erfolgreich korrigiert haben, wird die Liste aktualisiert und Ihr System aus der Liste entfernt. Anderenfalls verbleiben die nicht konformen Systeme in der Liste.
6. Klicken Sie zum Abschluss auf **Fertigstellen**.

Herunterladen eines ISO für manuelle Firmware-Aktualisierungen

Das OpenManage Integration for VMware vCenter repariert automatisch die meisten Konformitätsfehler. In manchen Fällen ist eine manuelle ISO-Installation erforderlich. Sie können die benötigte ISO zum manuellen Reparieren der Konformität durch die folgenden Schritte herunterladen:

1. Klicken Sie zum Herunterladen eines ISO im **Dell Management Center** → **Konformität** → **Bare-Metal-Server** auf **ISO herunterladen**.
2. Suchen Sie im Dialogfeld **ISO herunterladen** den Speicherort des ISO und klicken Sie auf **Herunterladen**.

   ANMERKUNG: Der externen Browser wird eventuell hinter diesem Anwendungsfenster geöffnet.
3. Suchen Sie die ISO-Datei, die Sie benötigen, damit Ihre Bare-Metal-Server konform sind.
4. Brennen Sie das ISO-Image, starten Sie den Host über die ISO-Datei, und aktualisieren Sie anschließend die Komponenten auf die erforderliche Firmwareebene.

iDRAC-Lizenzkonformität

Wenn Sie die Seite „iDRAC-Lizenzkonformität" auswählen, wird ein Konformitätstest ausgeführt. Dieser Test dauert einige Minuten. Die auf der Seite aufgeführten vSphere-Hosts und Bare-Metal-Servers sind nicht konform, da sie keine kompatible iDRAC-Lizenz aufweisen. Die Tabelle zeigt den Status der iDRAC-Lizenz an. Außerdem können Sie auf dieser Seite die verbleibende Gültigkeitsdauer der Lizenz anzeigen und sie ggf. aktualisieren. Wenn Ihr *Bestandsaufnahme-Job ausführen*-Link deaktiviert ist, so sind laut iDRAC-Lizenz keine vSphere-Hosts mehr konform. Wenn der *Konformität der*

Bare-Metal-Server erneut überprüfen-Link deaktiviert ist, so bedeutet dies, dass laut iDRAC-Lizenz keine Bare-Metal-Server mehr konform sind.

1. Klicken Sie im linken Fensterbereich des **Dell Management Center** auf **Konformität**.
2. Erweitern Sie **Konformität** und klicken Sie auf **iDRAC-Lizenzen**.

   Nachdem Sie diese Seite aufgerufen haben, wird der Konformitätstest ausgeführt. Dies ist der gleiche Test, der ausgeführt wird, wenn Sie auf **Aktualisieren** klicken.
3. Wenn Ihre Lizenz abgelaufen ist, klicken Sie auf **iDRAC-Lizenz erwerben/erneuern**.
4. Melden Sie sich bei der Seite **Dell License Management** an und aktualisieren oder erwerben Sie eine neue iDRAC-Lizenz.

   Verwenden Sie die Informationen auf dieser Seite, um Ihren iDRAC zu identifizieren und zu aktualisieren.
5. Nachdem Sie eine iDRAC-Lizenz installiert haben, fühen Sie die Aufgabe zum Erstellen einer Bestandsaufnahme für vSphere-Hosts aus und kehren zu dieser Seite zurück, nachdem die Aufgabe zum Erstellen der Bestandsaufnahme abgeschlossen ist. Bei Bare-Metal-Servern prüfen Sie erneut die Konformität der lizenzierten Bare-Metal-Server.

OpenManage Integration for VMware vCenter aktualisieren

Das folgende Szenario ist für die Aktualisierung von OpenManage Integration for VMware vCenter:

- Aktualisieren von einer Testversion auf eine Vollversion des Produkts

ANMERKUNG: Führen Sie ein Geräte-Backup durch, bevor Sie die Aktualisierung beginnen. Lesen Sie dazu Ausführen eines sofortigen Backups.

Aktualisieren von einer Testversion auf eine Vollversion des Produkts

So führen Sie eine Aktualisierung von einer Testversion auf eine Vollversion des Produkts durch:

1. Rufen Sie die **Dell-Website** auf und erwerben Sie die Produkt-Vollversion.

   Sie können auch in OpenManage Integration for VMware vCenter auf die Dell-Website zugreifen, indem Sie einen der **Jetzt kaufen**-Links verwenden, wie z.B. den im Fenster **Lizenzierung** des Verwaltungsportals. Dies gilt nur, wenn Sie eine Test-Lizenz verwenden.
2. Der Download umfasst die neue, vollständige Produktversion sowie eine neue Lizenzdatei.
3. Öffnen Sie ein Browser-Fenster und geben Sie die **Verwaltungskonsolen-URL** ein, die auf der Registerkarte **vSphere vCenter Console** der zu konfigurierenden virtuellen Maschine angezeigt wird oder verwenden Sie den Link auf der Seite **Dell Management Console** → **Einstellungen**. Die URL hat die folgende Syntax und ist unabhängig von der Groß-/Kleinschreibung: **https://<GeräteIPAdresse>**
4. Geben Sie im Anmeldefenster der **Verwaltungskonsole** das Kennwort ein und klicken Sie auf **Anmelden**.
5. Klicken Sie zum Hochladen der Lizenzdatei auf **Hochladen**.
6. Klicken Sie zum Suchen der Lizenzdatei im Fenster **Lizenz hochgeladen** auf **Durchsuchen**.
7. Wählen Sie die Lizenzdatei aus und klicken Sie auf **Hochladen**.

Informationen über die OpenManage Integration for VMware vCenter-Lizenzierung

Die OpenManage Integration for VMware vCenter verfügt über zwei Arten von Lizenzen:

Test-Lizenz Die Test-Lizenz beinhaltet eine Demo-Lizenz für fünf Hosts (Server), die durch OpenManage Integration for VMware vCenter verwaltet werden. Dies gilt nur für die 11. und höhere Generationen. Dies ist eine Standardlizenz und gilt für einen Zeitraum von 90 Tagen.

Produkt-Lizenz	Die Produkt-Vollversion enthält eine Standardlizenz für bis zu zehn vCenter und die erworbene Anzahl an Hostverbindungen, die vom OpenManage Integration for VMware vCenterverwaltet werden.

Wenn Sie von einer Test-Lizenz zu einer Produkt-Lizenz erweitern, wird Ihnen eine neue XML-Datei per E-Mail zugesendet. Speichern Sie die Datei auf Ihrem lokalen System und laden Sie die neue Lizenzdatei unter Verwendung der Administration Console hoch. Die Lizenzierung zeigt die folgenden Informationen an:

- Höchstzahl der vCenter-Verbindungslizenzen – bis zu zehn registrierte und verwendete vCenter-Verbindungen sind zulässig.
- Höchstzahl der Host-Verbindungslizenzen – die Anzahl an erworbenen Lizenzen für Hostverbindungen.
- In Verwendung – die Anzahl an Lizenzen für vCenter-Verbindungen oder Hostverbindungen. Bei Hostverbindungen steht diese Zahl für die Anzahl an Hosts (oder Servern) die erfasst und in die Bestandsliste aufgenommen wurden.
- Verfügbar – die Anzahl an Lizenzen für vCenter-Verbindungen oder Hostverbindungen, die für die Nutzung zur Verfügung stehen.
- Nicht lizenzierte Hosts – die Anzahl an Hostverbindungen, die die lizenzierte Menge überschreiten. Die OpenManage Integration for VMware vCenter arbeitet weiter normal, es muss jedoch eine neue Lizenz erworben und installiert werden, um diese Warnmeldung zu entfernen.

4

End-To-End Hardware-Verwaltung

Das Ziel der End-to-End Hardware-Verwaltung besteht darin, Informationen zum Systemzustand und zur aktuellen Infrastruktur bereitzustellen, die der Administrator benötigt, um auf kritische Hardware-Ereignisse zu reagieren, ohne das Dell Management Center oder das vCenter zu verlassen. Die End-to-End Hardware-Verwaltung innerhalb des OpenManage Integration for VMware vCenterist in vier separate Bereiche unterteilt:

- Überwachung
- Bestandsaufnahme
- Erweiterte Hostverwaltung
- Garantieabfrage

Überwachen des Datencenter- und des Hostsystems

Mit der Datacenter- und Hostsystemüberwachung kann ein Administrator den Funktionszustand der Infrastruktur überwachen, indem die Hardware- (Server und Massenspeicher) und Virtualisierungs-bezogenen Ereignisse auf der Registerkarte „Tasks und Ereignisse" in vCenter angezeigt werden. Darüber hinaus werden wichtige Hardware-Warnungen die OpenManage Integration for VMware vCenter-Alarme auslösen. Nur wenige für Dell Virtualisierungsbezogene definierte Ereignisse können das verwaltete Host-System in den Wartungsmodus bringen.

So führen Sie eine Überwachung durch:

1. Konfigurieren Sie die Einstellungen für **Ereignisse und Alarme**.
2. Konfigurieren von **SNMP-OMSA-Trap-Zielen**, falls erforderlich.
3. Überprüfen Sie die Ereignisinformationen auf der Registerkarte **Tasks und Ereignisse**.

Ereignisse und Alarme

Sie können Ereignisse und Alarme von dem OpenManage Integration for VMware vCenter auf der Registerkarte **Verwalten** → **Einstellungen** bearbeiten. Von hier können Sie die Ereignisanzeigeebene auswählen, die Alarme für Dell Hosts aktivieren oder Standardalarme wiederherstellen. Sie können Ereignisse oder Alarme für einzelne vCenter oder alle registrierten vCenter gleichzeitig konfigurieren.

Es gibt vier Ereignis-Veröffentlichungsstufen.

Tabelle 1. Beschreibung der Ereignis-Veröffentlichungsstufen

Ereignis	Beschreibung
Keine Ereignisse anzeigen	OpenManage Integration for VMware vCenter soll keine Ereignisse oder Alarme an betroffene vCenter weiterleiten.
Alle Ereignisse anzeigen	Anzeigen aller Ereignisse, einschließlich informeller Ereignisse, die das OpenManage Integration for VMware

	vCenter von den verwalteten Dell Hosts der betroffenen vCenter erhält.
Nur kritische Ereignisse und Warnungsereignisse anzeigen	Veröffentlicht nur kritische Ereignisse und Warnungen an die entsprechenden vCenter.
Nur kritische Ereignisse und Warnungsereignisse hinsichtlich der Visualisierung anzeigen.	Veröffentlicht von Hosts empfangene Virtualisierung-bezogene Ereignisse an die entsprechenden vCenter. Virtualisierung-bezogene Ereignisse sind solche Ereignisse, in denen Dell für Hosts, die virtuelle Maschinen ausführen, die höchste Priorität zugewiesen hat.

Wenn Sie Ereignisse und Alarme konfigurieren, können Sie sie aktivieren. In diesem Fall führen kritische Hardware-Alarme dazu, dass das OpenManage Integration for VMware vCenterdas Hostsystem in den Wartungsmodus versetzt und die virtuellen Maschinen in bestimmten Fällen auf ein anderes Hostsystem migriert. Das OpenManage Integration for VMware vCenter leitet die von verwalteten Dell-Hosts empfangenen Ereignisse weiter und erstellt Alarme für diese Ereignisse. Sie können diese Alarme dazu verwenden, Aktionen des vCenter wie einen Neustart, den Wartungsmodus oder eine Migration zu veranlassen. Beispiel: Wenn eine duale Netzversorgung ausfällt und ein Alarm erzeugt wird, kann die virtuelle Maschine auf diesem Host auf einen anderen migriert werden.

Ein Host wechselt nur auf Anforderung in den oder aus dem Wartungsmodus. Befindet sich der Host beim Eintritt in den Wartungsmodus in einem Cluster, haben Sie die Möglichkeit, ausgeschaltete virtuelle Maschinen zu evakuieren. Ist diese Option ausgewählt, wird jede ausgeschaltete virtuelle Maschine auf einen anderen Host migriert, es sei denn, im Cluster steht kein kompatibler Host für die virtuelle Maschine zur Verfügung. Im Wartungsmodus erlaubt der Host keine Bereitstellung bzw. kein *Einschalten* einer virtuellen Maschine. Virtuelle Maschinen, die auf einem Host ausgeführt werden, der in den Wartungsmodus eintritt, werden entweder manuell oder automatisch vom VMware Distributed Resource Scheduling (DRS) auf einen anderen Host migriert oder heruntergefahren.

Alle Hosts außerhalb oder innerhalb der Cluster ohne aktiviertes VMware Distributed Resource Scheduling (DRS) können virtuelle Maschinen sehen, die aufgrund eines kritischen Ereignisses heruntergefahren werden. Das DRS überwacht die Nutzung kontinuierlich über einen Ressourcen-Pool und teilt verfügbare Ressourcen gemäß den Geschäftsanforderungen intelligent zwischen den virtuellen Maschinen auf. Verwenden Sie Cluster mit konfiguriertem DRS zusammen mit Dell-Alarmen, um sicherzustellen, dass virtuelle Maschinen bei kritischen Hardware-Ereignissen automatisch migriert werden. In den Details der Bildschirm-Meldungen werden alle eventuell betroffenen Cluster in dieser vCenter-Instanz aufgeführt. Bestätigen Sie, dass die Cluster betroffen sind, bevor Sie Ereignisse und Alarme aktivieren.

Wenn Sie die Standard-Alarmeinstellungen wiederherstellen müssen, können Sie auf die Schaltfläche „Reset Default Alarm" (Standard-Alarmeinstellungen wiederherstellen) klicken. Mit dieser Schaltfläche kann die standardmäßige Alarm-Konfiguration wiederhergestellt werden, ohne dass das Produkt de- und neuinstalliert werden muss. Alle nach der Installation geänderten Dell-Alarm-Konfigurationen werden durch Klicken auf diese Schaltfläche auf die Standardeinstellung zurückgesetzt.



ANMERKUNG: Um Dell Ereignisse zu erhalten, müssen Sie die Ereignisse aktivieren.



ANMERKUNG: Das OpenManage Integration for VMware vCenter trifft eine Vorauswahl der erforderlichen Virtualisierung-bezogenen Ereignisse, damit Hosts virtuelle Maschinen erfolgreich ausführen können. Die Dell-Host Alarme sind in der Standardeinstellung deaktiviert. Wenn die Dell-Alarme aktiviert werden, sollten die Cluster das VMware Distributed Resource Scheduling verwenden, um sicherzustellen, dass virtuelle Maschinen, die kritische Ereignisse senden, automatisch migriert werden.

Grundsätzliches zu OMSA für Hosts der 11. Generation von Dell PowerEdge

Auf Servern vor der 12. Dell PowerEdge-Generation muss OMSA installiert werden, damit OpenManage Integration for VMware vCenter ordnungsgemäß funktioniert. OMSA wird im Rahmen der Bereitstellung auf Dell PowerEdge-Hosts der

11. Generation automatisch installiert, Sie können jedoch immer noch eine manuelle Installation durchführen, falls Sie dies wünschen.

 **ANMERKUNG:** Durch Bereitstellung des OMSA-Agenten unter Verwendung des OpenManage Integration for VMware vCenter startet dieses den httpClient-Dienst, aktiviert den Port 8080 und gibt ihn nach ESXi 5.0 frei, um OMSA VIB herunterzuladen und zu installieren. Sobald die OMSA-Installation abgeschlossen wurde, wird der Dienst automatisch angehalten und der Port wird geschlossen.

Wählen Sie für die Konfiguration von OMSA auf Dell PowerEdge-Servern der 11. Generation unter den folgenden Optionen aus:

- Bereitstellen eines OMSA-Agenten auf einem ESXi-System
- Bereitstellen eines OMSA-Agenten auf einem ESX-System
- Einrichten eines OMSA-Trap-Ziels

Bereitstellen eines OMSA-Agenten auf einem ESX-System

Installieren Sie die OMSA-Datei tar.gz auf einem ESX-System, um eine Bestandsliste und Alarminformationen der Systeme zu erstellen.

 **ANMERKUNG:** OpenManage-Agenten sind auf Dell-Hosts vor den Dell PowerEdge-Servern der 12. Generation erforderlich. Installieren Sie OMSA unter Verwendung von OpenManage Integration for VMware vCenter oder installieren Sie es manuell auf Hosts, bevor Sie die OpenManage Integration for VMware vCenter installieren. Details über die manuelle Installation der Agenten finden Sie unter **http://en.community.dell.com/techcenter/systems-management/w/wiki/1760.openmanage-server-administrator-omsa.aspx.**

So stellen Sie die OMSA-Agent-Datei tar.gz auf einem ESX-System mit der erforderlichen Remote-Aktivierungseinstellung (-c) bereit:

1. Führen Sie das OMSA-Agent-Installationsskript aus:
   ```
   srvadmin-install.sh -x -c
   ```
2. Starten Sie die OMSA-Dienste:
   ```
   srvadmin-services.sh start
   ```
3. Wenn der OMSA-Agent bereits installiert wurde, stellen Sie sicher, dass die Remote-Aktivierungseinstellung (-c) konfiguriert ist, anderenfalls kann die Installation des OpenManage Integration for VMware vCenter nicht erfolgreich abgeschlossen werden. Installieren Sie sie mit der Option -c erneut und starten Sie den Dienst neu:
   ```
   srvadmin-install.sh -c srvadmin-services.sh restart
   ```

Bereitstellen eines OMSA-Agenten auf einem ESXi-System

Installieren Sie den OMSA VIB auf einem ESXi-System, um eine Bestandsliste und Alarminformationen von den Systemen zu erstellen.

 **ANMERKUNG:** OpenManage-Agenten sind auf Dell-Hosts vor den Dell PowerEdge-Servern der 12. Generation erforderlich. Installieren Sie OMSA unter Verwendung von OpenManage Integration for VMware vCenter oder installieren Sie es manuell auf Hosts, bevor Sie die OpenManage Integration for VMware vCenter installieren. Details über die manuelle Installation der Agenten finden Sie unter **http://en.community.dell.com/techcenter/systems-management/w/wiki/1760.openmanage-server-administrator-omsa.aspx.**

1. Falls noch nicht geschehen, installieren Sie das vSphere-Befehlszeilentool (vSphere CLI) von **http://www.vmware.com**.
2. Geben Sie folgenden Befehl ein:
   ```
   Vihostupdate.pl -server <IP Address of ESXi host> -i -b OM-SrvAdmin-Dell-Web-6.3.0-2075.VIB-ESX41i_A00.8.zip
   ```
    **ANMERKUNG:** Die Installation von OMSA kann einige Minuten dauern. Dieser Befehl erfordert einen Neustart des Hosts nach Abschluss der Installation.

Einrichten eines OMSA-Trap-Ziels

Auf allen Servern der 11. Generation von Hosts muss OMSA konfiguriert sein.

ANMERKUNG: OMSA ist nur auf Dell-Servern vor Dell PowerEdge-Servern der 12. Generation erforderlich.

So richten Sie ein OMSA-Trap-Ziel ein:

1. Verwenden Sie entweder den Link zur OMSA-Benutzeroberfläche unter **Einstellungen** → **Allgemein**, oder rufen Sie den OSMA-Agenten in einem Webbrowser auf (**https://<HostIP>:1311/**).
2. Melden Sie sich an und wählen Sie die Registerkarte **Alarmverwaltung**.
3. Wählen Sie **Alarm-Aktionen** und stellen Sie sicher, dass die Option **Broadcast-Nachricht** für alle zu überwachenden Ereignisse gesetzt ist, so dass die Ereignisse gesendet werden.
4. Wählen Sie oben auf der Registerkarte die Option **Plattform-Ereignisse**.
5. Klicken Sie auf die graue Schaltfläche **Ziele konfigurieren** und dann auf den Link **Ziel**.
6. Aktivieren Sie das Kontrollkästchen **Ziel aktivieren**.
7. Geben Sie die OpenManage Integration for VMware vCenter Geräte-IP-Adresse in das **Feld Ziel-IP-Adresse** ein.
8. Klicken Sie auf **Änderungen anwenden**.
9. Wiederholen Sie die Schritte 1 bis 8, um weitere Ereignisse zu konfigurieren.

Anzeigen von Ereignissen

Führen Sie zum Anzeigen von Ereignissen einen der folgenden Schritte aus:

- Navigieren Sie zur virtuellen Maschine und klicken Sie mit der rechten Maustaste, um die Registerkarte **vCenter** → **Tasks und Ereignisse** anzuzeigen. Klicken Sie dann auf **Ereignisse**, um die ausgewählte Ereignisebene anzuzeigen.
- Klicken Sie auf den übergeordneten Knoten (Cluster oder Datacenter) des Hosts oder des Root-Ordners des vCenter.

Ereignisse werden nur für die Knoten in der vSphere-Struktur angezeigt.

vSphere-Client Host – Übersicht

Die Übersicht enthält Informationen zu wichtigen Hostserver-Attributen, einschließlich des Zustands der einzelnen Komponenten sowie Identifikations-, Hypervisor- und Firmware-Informationen.

STATUS DER HARDWAREKOMPONENTE

Der Zustand der Hardwarekomponenten ist eine grafische Darstellung des Status der wichtigsten Hostserverkomponenten: Systemgehäuse, Netzteile, Temperatur, Lüfter, Spannung, Prozessoren, Batterien, Eingriff, Hardwareprotokoll, Stromverwaltung und Speicher. Die Komponenten können folgenden Status aufweisen:

- Funktionsfähig (grünes Häkchen) – Komponente arbeitet normal
- Warnung (gelbes Dreieck mit Ausrufezeichen) – Komponente weist einen nichtkritischen Fehler auf
- Kritisch (rotes X) – Komponente weist einen kritischen Fehler auf
- Unbekannt (Fragezeichen) – der Status der Komponente ist unbekannt

Der globale Funktionsstatus wird in der Kopfzeile oben rechts angezeigt.

SERVER-INFORMATIONEN

Die Server-Informationen umfassen Identifikations-, Hypervisor- und Firmware-Informationen wie:

- Hostname, Stromzustand, iDRAC-IP-Adresse, Management-IP-Adresse, verwendetes Verbindungsprofil, Modell, Service-Tag- und Asset-Tag-Nummern, verbleibende Garantiezeit in Tagen und Datum des letzten Bestandsaufnahme-Scans.
- Versionen von Hypervisor, BIOS-Firmware und iDRAC-Firmware.
- Die zehn aktuellsten Systemereignisprotokolleinträge. Klicken Sie zum Aufrufen des Fensters „Systemereignisprotokoll“, das zusätzliche Protokolldetails enthält, auf „Details“.

Hostinformationen

Im linken Fensterbereich der Host-Übersicht finden Sie Links zu den folgenden Hostinformationen:

- System-Ereignisprotokoll

  Zeigt Informationen aus dem Hardwaresystem-Ereignisprotokoll an. Lesen Sie dazu Systemereignisprotokolle.
- Hardware-Bestandsaufnahme

  Zeigt Informationen zu den folgenden Hardware-Geräten an:

  - Austauschbare Funktionseinheiten (Field-replaceable units, FRUs) – DIMMS, Systemplanar, Netzteile, Rückwandplatinen, Controllerkarten usw.
  - Speicher – die Anzahl der verfügbaren und belegten Steckplätze, die maximale Kapazität und die Menge des belegten Speichers sowie die Details zu den einzelnen DIMM-Modulen.
  - Netzwerkschnittstellenkarten (NICs) – die Anzahl der installierten Karten und Details zu den einzelnen NICs.
  - PCI-Steckplätze – Insgesamt verfügbare und belegte Steckplätze sowie Details zu den einzelnen Steckplätzen.
  - Netzteile – Anzahl der vorhandenen Netzteile sowie Details zu den einzelnen PSUs.
  - Prozessoren – Anzahl der vorhandenen Prozessoren sowie Details zu den einzelnen CPUs.
  - Remote-Zugriffskarte – IP-Adressinformationen, RAC-Typ sowie URL der Webschnittstelle.

  Lesen Sie dazu Allgemeines zu Bestandsaufnahme-Jobs.
- Bei Lagerung

  Der Hostsystem-Speicher bietet eine grafische und detaillierte Ansicht der Kapazität und Art des physikalischen und logischen Speichers für Speichergeräte, die an einen Host-basierten Speicher-Controller angeschlossen sind:

  - Gesamter Speicherplatz des Hostsystems, unkonfiguriert, konfiguriert und Kapazität der globalen und dedizierten Hotspare-Festplatten
  - Führt auf, wie viele Teile jeder Speicherkomponente in der Datentabelle der Systemkomponenten vorhanden sind, die ausführliche Informationen zu dieser Komponente enthält
- Firmware

  Führt den Assistenten zur Firmware-Aktualisierung aus oder zeigt die Version Ihrer Firmware an. Lesen Sie dazu Firmware-Aktualisierungen.
- Stromüberwachung

  Die Leistungsüberwachung des Hostsystems bietet allgemeine Informationen zur Stromversorgung, Energie-Statistiken sowie Informationen zur Leistungsreserve, einschließlich:

  - Aktuelles Leistungsbudget, Profil-, Warn- und Ausfallgrenzwerte
  - Statistiken zur Leistungsaufnahme, System-Spitzenleistung sowie zur Stromstärke
  - Reserveleistung und Spitzenreservekapazität

  ANMERKUNG: Diese Funktion wird nicht von allen Netzteilen unterstützt. Netzteile aus dem Blade-Gehäuse werden nicht unterstützt.
- Garantie

  Die Garantieabfrage bietet die folgenden Informationen zu Dell-Servern:

  - Aktualisierte Servicegarantie-Informationen durch Übertragen der Service-Tag-Nummer des Hosts
  - Garantieinformationen, die in festgelegten Intervallen aktualisiert werden
  - Sichere Übertragung dank Proxyserver und Berechtigungsnachweis
  - Informationen über eine getestete, sichere Verbindung.

  Lesen Sie dazu Garantieabfrage.

Hostmaßnahmen

Hostmaßnahmen sind Befehle, die Sie am aktuellen Hostserver ausführen können. Beispiele:

- Verwenden Sie „Anzeige aufblinken lassen“, um die Anzeigeleuchte am LCD aufblinken zu lassen. Lesen Sie dazu Einrichten der Anzeigeleuchten an der Frontblende eines physischen Servers.
- Verwenden Sie „Assistent zur Firmware-Aktualisierung ausführen“, um den Assistenten anzuzeigen und die Hostserver-Firmware zu aktualisieren. Lesen Sie dazu Ausführen des Assistenten zur Firmware-Aktualisierung.
- Verwenden Sie das iDRAC-Reset, um das iDRAC ohne einen Neustart des Hosts neu zu starten. Lesen Sie dazu iDRAC-Reset durchgeführen .

Management-Konsolen

Die Management-Konsolen dienen zum Starten der externen System Management-Konsolen. Dazu gehören:

- Klicken Sie auf „Remote-Zugriff-Konsole“, um die Web-Benutzeroberfläche von Integrated Dell Remote Access Controller (iDRAC) zu starten.
- Klicken Sie auf „OMSA-Konsole“, um die Benutzeroberfläche von OpenManage Server Administrator (OMSA) zu starten, sofern diese konfiguriert wurde. Lesen Sie dazu Aktivieren des OMSA-Links
- Klicken Sie auf „Blade-Gehäuse-Konsole“, um die Web-Benutzeroberfläche „Chassis Management Controller“ (CMC) zu starten.

Dell Online Services

Durchführen des iDRAC-Resets

Manchmal reagiert iDRAC nicht mehr auf Anfragen und dies führt zu unerwartetem Verhalten innerhalb des OpenManage Integration for VMware vCenter Der einzige Weg zur Wiederherstellung aus diesem Zustand ist der iDRAC-Reset. Ein iDRAC-Reset führt einen normalen Neustart des iDRACs durch. Dieser Neustart startet den Host nicht neu. Es dauert 1-2 Minuten, nachdem Sie den Reset durchgeführt haben, bis iDRAC in einen verwendbaren Zustand zurückkehrt.

Während der Neustart des iDRACs durchgeführt wird, sehen Sie eventuell folgende Meldungen:

- Es ist eine Verzögerung oder ein Kommunikationsfehler aufgetreten, während OpenManage Integration for VMware vCenter seinen Funktionszustand abgerufen hat.
- Alle mit iDRAC geöffneten Sitzungen werden geschlossen.
- Die DHCP-Adresse für den iDRAC wird eventuell geändert. Sollte iDRAC DHCP für seine IP-Adressen verwenden, besteht die Chance, dass die IP-Adresse geändert wird. In diesem Fall führen Sie den Host-Bestandsaufnahme-Job erneut aus, um die neue iDRAC-IP in den Bestandsaufnahmedaten zu erfassen.

ANMERKUNG: Ein Software-Reset des iDRACs funktioniert möglicherweise nicht immer, um den iDRAC wieder zurück in einen verwendbaren Zustand zu versetzen. Möglicherweise müssen Sie einen Hard-Reset durchführen. Zum Durchführen eines Hard-Resets des Servers schalten Sie den Server aus, ziehen Sie das Netzkabel für Minuten ab, und schließen Sie es wieder an. Beziehen Sie sich für weitere Informationen über das Zurücksetzen des iDRACs auf Ihre Version des iDRAC-Benutzerhandbuchs.

ANMERKUNG: Dell empfiehlt, dass Sie den Host in den Wartungsmodus versetzen, bevor Sie den iDRAC-Reset durchführen.

1. Wählen Sie im **vSphere-Client** unter der Überschrift **Bestandsaufnahme** die Option **Hosts und Cluster** aus.
2. Wählen Sie unter **Hosts und Cluster** das Hostsystem in der Baumstruktur aus und klicken Sie auf die Registerkarte **OpenManage Integration**.
3. Wählen Sie unter **Host-Aktionen iDRAC-Reset** aus.
4. Im Dialogfeld „iDRAC-Reset“ wählen Sie **iDRAC-Reset fortsetzen** aus und klicken Sie auf **OK**.

Allgemeines zu Bestandsaufnahmenplänen

Der Bestandsaufnahmenplan legt einen Tag/eine Uhrzeit für das Ausführen von Jobs zum Erstellen von Bestandsaufnahmen fest. Beispiele:

- Wöchentlich zu einer bestimmten Uhrzeit und an bestimmten Tagen
- In einem bestimmten Zeitintervall

Die meisten Funktionen des OpenManage Integration for VMware vCenter erfordern, dass zuerst eine Bestandsaufnahme abgeschlossen wird, um erforderliche Daten zu sammeln. Zum Anzeigen dieser Informationen muss eine Bestandsaufnahme aller Hostsysteme erstellt werden. Zum Erstellen einer Bestandsaufnahme der Hostsysteme müssen Sie ein Verbindungsprofil erstellen, das Verbindungs- und Authentifizierungsinformationen bereitstellt. Wenn die Bestandsaufnahme vollständig ist, können Sie die Ergebnisse der Bestandsaufnahme für das gesamte Datacenter oder ein einzelnes Hostsystem anzeigen.



ANMERKUNG: Um sicherzustellen, dass die Bestandsaufnahme aktuelle Informationen enthält, sollten Sie das Erstellen einer Bestandsaufnahme mindestens einmal wöchentlich planen. Das Erstellen einer Bestandsaufnahme erfordert nur minimale Ressourcen und wirkt sich nicht negativ auf die Hostleistung aus.

Verwandte Aufgaben:

- Ausführen von Bestandsaufnahme-Jobs
- Modifizieren eines Zeitplans zum Erstellen einer Bestandsaufnahme
- Anzeigen der Bestandsaufnahme eines einzelnen Hostsystems
- Anzeigen der Konfiguration und des Status der Datacenter-Hardware

Modifizieren eines Zeitplans zum Erstellen einer Bestandsaufnahme

Der Bestandsaufnahme-Plan legt einen Tag/eine Uhrzeit für das Ausführen von Jobs zum Erstellen von Bestandsaufnahmen fest. Beispiele:

- Wöchentlich zu einer bestimmten Uhrzeit und an bestimmten Tagen.
- In einem vorgegebenen Zeitintervall muss eine vollständige Bestandsaufnahme erstellt werden, um Daten zu sammeln, die für einen Großteil der Funktionen im OpenManage Integration for VMware vCenter erforderlich sind.



ANMERKUNG: Um sicherzustellen, dass die Bestandsaufnahme aktuelle Informationen enthält, sollten Sie das Erstellen einer Bestandsaufnahme mindestens einmal wöchentlich planen. Der Bestandsaufnahme-Job erfordert nur minimale Ressourcen und wirkt sich nicht negativ auf die Hostleistung aus.

So modifizieren Sie einen Zeitplan zum Erstellen einer Bestandsaufnahme:

1. Wählen Sie im Dell Management Center die Option **Einstellungen** → **Zeitplan Bestandsaufnahme** aus.
2. Klicken Sie auf **Bearbeiten**, um den aktuellen Zeitplan zu bearbeiten.
3. Wählen Sie das Optionsfeld **An ausgewählten Tagen**, dann aktivieren Sie das Kontrollkästchen für den Wochentag und geben die Uhrzeit ein. Klicken Sie auf **Löschen**, um die Einträge zu löschen.
4. Klicken Sie auf **Übernehmen**, um den Bestandsaufnahmezeitplan zu ändern, oder klicken Sie auf **Abbrechen**, um den Vorgang abzubrechen.
5. Wählen Sie im Management Center **Job-Warteschlange** und die Registerkarte **Bestandslistenverlauf** aus, um den Job sofort auszuführen.
6. Klicken Sie auf **Jetzt ausführen**.
7. Klicken Sie zum Aktualisieren der **Details der letzten Bestandsaufnahme-Jobs** auf **Aktualisieren**.

Anzeigen der Bestandsaufnahme eines einzelnen Hostsystems in vCenter

So zeigen Sie die Bestandsaufnahme für ein einzelnes Hostsystem an:

1. Wählen Sie im **vSphere-Client** unter der Überschrift **Bestandsaufnahme** die Option **Hosts und Cluster** aus.
2. Wählen Sie im linken Fensterbereich von **Hosts und Cluster** das Hostsystem aus und klicken Sie auf die Registerkarte **OpenManage Integration**.
3. Eine Übersicht des ausgewählten Hosts wird angezeigt.

   Die Übersicht enthält Informationen zu wichtigen Hostserver-Attributen, einschließlich des Zustands der einzelnen Komponenten, Identifikations-, Hypervisor- und Firmware-Informationen.

   - Der Zustand der Hardwarekomponenten ist eine grafische Darstellung des Status der wichtigsten Hostserverkomponenten: Systemgehäuse, Netzteile, Temperatur, Lüfter, Spannung, Prozessoren, Batterien, Eingriff, Hardwareprotokoll, Stromverwaltung und Speicher. Die Komponenten können folgenden Status aufweisen:

     – Funktionsfähig (grünes Häkchen) – Komponente arbeitet normal

     – Warnung (gelbes Dreieck mit Ausrufezeichen) – Komponente weist einen nichtkritischen Fehler auf

     – Kritisch (rotes X) – Komponente weist einen kritischen Fehler auf

     – Unbekannt (Fragezeichen) – der Status der Komponente ist unbekannt

     Der globale Funktionsstatus wird in der Kopfzeile oben rechts angezeigt.

   - Die Server-Informationen umfassen Identifikations-, Hypervisor- und Firmware-Informationen wie:

     – Hostname, Betriebszustand, iDRAC-IP-Adresse, Management-IP-Adresse, verwendetes Verbindungsprofil, Modell, Service-Tag- und Asset-Tag-Nummern, verbleibende Garantiezeit in Tagen und Datum des letzten Bestandslistenscans

     – Versionen von Hypervisor, BIOS-Firmware und iDRAC-Firmware

     – Fault Resilient Memory (FRM): Dies ist ein BIOS-Attribut und wird in BIOS während dem ersten Einrichten des Servers aktiviert und zeigt den Speicherbetriebsmodus auf dem Server an. Wenn Sie die Speicherbetriebsmodus-Werte ändern, müssen Sie Ihr System neu starten. Dies gilt für **R620-**, **R720-**, **T620-**, **M620-**Server mit ESXi 5.5-Version oder höher. Die vier verschiedenen Werte sind:

       * Aktiviert und geschützt: Dieser Wert bedeutet, dass das System unterstützt wird und das Betriebssystem-Version ESXi 5.5 oder höher ist sowie, dass der Speicherbetriebsmodus in BIOS auf FRM eingestellt ist.

       * Aktiviert und nicht geschützt: Dieser Wert weist darauf hin, dass der Betriebsmodus der Speichermodule im BIOS auf FRM eingestellt wurde, das Betriebssystem diese Funktion aber nicht unterstützt.

       * Deaktiviert: Dieser Wert zeigt an, dass gültige Systeme mit jeglichen Betriebssystem-Versionen unterstützt werden und der Speicherbetriebsmodus in BIOS nicht auf FRM gesetzt ist.

       * Leer: Wenn der Speicherbetriebsmodus in BIOS nicht unterstützt wird, wird das FRM-Attribut nicht angezeigt.

   - Die „Letzte Systemprotokolleinträge“ enthalten die zehn aktuellsten Systemereignisprotokolleinträge. Klicken Sie zum Aufrufen des Fensters **Systemereignisprotokoll**, das zusätzliche Protokolldetails enthält, auf **Details**.
4. Klicken Sie unter **Hostinformationen** auf **Hardware-Bestandsaufnahme**, um eine Liste und weitere Einzelheiten zu den im Hostsystem installieren Komponenten anzuzeigen. Dazu gehören:

   - Austauschbare Funktionseinheiten (Field-replaceable units, FRUs) – DIMMS, Systemplanar, Netzteile, Rückwandplatinen, Controllerkarten usw.

- Speicher – die Anzahl der verfügbaren und belegten Steckplätze, die maximale Kapazität und die Menge des belegten Speichers sowie die Details zu den einzelnen DIMM-Modulen.
- Netzwerkschnittstellenkarten (NICs) – die Anzahl der installierten Karten und Details zu den einzelnen NICs.
- PCI-Steckplätze – Insgesamt verfügbare und belegte Steckplätze sowie Details zu den einzelnen Steckplätzen.
- Netzteile – Anzahl der vorhandenen Netzteile sowie Details zu den einzelnen PSUs.
- Prozessoren – Anzahl der vorhandenen Prozessoren sowie Details zu den einzelnen CPUs.
- Remote-Zugriffskarte – IP-Adressinformationen, RAC-Typ sowie URL der Webschnittstelle.

5. Klicken Sie unter **Hostinformationen** auf **Speicher**, um eine Grafik und detaillierte Ansicht der Kapazität und des physischen und virtuellen Speichertyps anzuzeigen. Dazu gehören:

   - Gesamt-Speicherkapazität des Hostsystems, unkonfiguriert und konfiguriert sowie Kapazität der globalen Hotspare-Festplatte.
   - Eine Liste, wie viele Elemente jeder Speicherkomponente im System vorhanden sind.
   - Eine Tabelle mit den Komponentendaten, die detaillierte Informationen zu den einzelnen Komponenten enthält.

6. Klicken Sie unter **Hostinformationen** auf **Firmware**, um Informationen zur Firmware aller Dell Lifecycle Controller anzuzeigen. Dazu gehören:

   - Aktualisierungsname – BIOS, Dell Lifecycle Controller, Netzteil usw.
   - Aktualisierungstyp – BIOS, Firmware oder Anwendung.
   - Details individueller Aktualisierungen – Version, Installationszeit, ob eine Aktualisierung durchgeführt wird bzw. der Aktualisierungsstatus und die Aktualisierungsversion. Der Aktualisierungsstatus und die -version enthalten nur dann Daten, wenn eine Aktualisierung geplant ist. Die Aktualisierungsversion ist die Firmwareversion, auf die das System aktualisiert wird.

7. Klicken Sie unter **Hostinformationen** auf **Stromüberwachung**, um allgemeine Informationen zur Stromversorgung, den Energiestatistiken und Informationen zur Leistungsreserve anzuzeigen. Dazu gehören:

   - Aktuelles Leistungsbudget, Profil, Warn- und Fehlergrenzwerte.
   - Leistungsaufnahme, System-Spitzenleistung sowie Statistiken zur Stromstärke.
   - Reserveleistung und Spitzenreservekapazität.

8. Klicken Sie unter **Hostinformationen** auf **Garantie**, um Informationen zur Systemgarantie anzuzeigen. Dazu gehören:

   - Anbieter und Beschreibung der Garantie.
   - Start- und Enddaten sowie Restlaufzeit der Garantie in Tagen.
   - Status der Garantie (aktiv, abgelaufen) und Datum, wann die Garantieinformationen das letzte Mal aktualisiert wurden.

Bestandsaufnahme und Lizenzierung

Wenn Serverdaten weder abgerufen noch angezeigt werden können, gibt es mehrere mögliche Ursachen:

- Dem Server wurde kein Verbindungsprofils zugewiesen, daher kann das Erstellen eines Bestandsaufnahme-Tasks nicht ausgeführt werden.
- Es wurde kein Bestandsaufnahme-Task auf dem Server ausgeführt, um die Daten zu erfassen. Somit können keine Daten angezeigt werden.
- Die Anzahl der Hostlizenzen wurde überschritten. Sie müssen zusätzliche Lizenzen erwerben, um einen Bestandsaufnahme-Task erstellen zu können.
- Der Server verfügt nicht über die erforderliche iDRAC-Lizenz für Server der 12. Generation und später. Sie müssen die korrekte iDRAC-Lizenz erwerben.

Der Link „Jetzt kaufen“ dient nur für den Erstkauf des Produkts und nicht für Aktualisierungen. Er wird nur dann angezeigt, wenn Sie eine Test-Lizenz verwenden.

Verwandte Aufgaben:

- Anzeigen und Bearbeiten eines bestehenden Verbindungsprofils
- Modifizieren eines Zeitplans zum Erstellen einer Bestandsaufnahme

OpenManage Integration for VMware vCenter verfügt über zwei Arten von Lizenzen:

- Test-Lizenz: Die Test-Lizenz beinhaltet eine Demo-Lizenz für fünf Host (Server), die durch OpenManage Integration for VMware vCenter verwaltet werden.
- Produkt-Lizenz: Die Produkt-Vollversion enthält eine Produktlizenz für drei vCenter und die erworbene Anzahl an Hostverbindungen, die vom OpenManage Integration for VMware vCenter verwaltet werden.

Verwandte Aufgaben:

- Informationen über die Dell OpenManage Integration for VMware vCenter-Lizenzierung
- Hochladen einer OpenManage Integration for VMware vCenter-Lizenz unter Verwendung der Administration Console

Anzeigen einer Speicher-Bestandsliste

Der Hostsystem-Speicher bietet eine grafische und detaillierte Ansicht der Kapazität und Art des physikalischen und logischen Speichers für Speichergeräte, die an einen Host-basierten Speicher-Controller angeschlossen sind:

- Gesamter Speicherplatz des Hostsystems, unkonfiguriert, konfiguriert und Kapazität der globalen Hotspare-Festplatten
- Eine Liste, wie viele Elemente jeder Speicherkomponente im System vorhanden sind
- Eine Tabelle mit den Komponentendaten, die detaillierte Informationen zu den einzelnen Komponenten enthält

So zeigen Sie die Speicherdaten an:

1. Wählen Sie im **vSphere-Client** einen Host aus und klicken Sie dann die auf Registerkarte **OpenManage Integration**.
2. Klicken Sie im linken Bereich auf der Seite **Host-Übersicht** auf **Speicher**.
3. Auf der Seite **Speicher** zeigen Sie eine graphische Übersicht an oder verwenden die Tabelle und die Dropdown-Listen **Ansicht** und **Filter**, um die Informationen in Ihrer Dropdown-Liste zu sortieren.

Anzeigen der Host-Stromüberwachung

Die Leistungsüberwachung des Hostsystems bietet allgemeine Informationen zur Stromversorgung, Energie-Statistiken sowie Informationen zur Leistungsreserve, einschließlich:

- Aktuelles Leistungsbudget, Profil-, Warn- und Ausfallgrenzwerte
- Statistiken zur Leistungsaufnahme, System-Spitzenleistung sowie zur Stromstärke
- Reserveleistung und Spitzenreservekapazität

So zeigen Sie die Host-Stromüberwachung an:

1. Wählen Sie im **vSphere-Client** Ihren Host aus und klicken Sie dann auf die Registerkarte **OpenManage Integration**.
2. Klicken Sie im linken Fensterbereich unter **Hostinformationen** auf **Stromüberwachung**.
3. Zeigen Sie auf der Seite **Stromüberwachung** die Leistungsdaten für diesen Host an.

Anzeigen der Konfiguration und des Status der gesamten Datacenter-Hardware

Bevor Sie die Konfiguration und den Status der gesamten Datacenter-Hardware anzeigen können, müssen Sie eine Bestandsliste erstellen. Nachdem Sie die Bestandsliste erstellt haben, können Sie folgende Elemente anzeigen:

- Hardware: Austauschbare Funktionseinheiten
- Hardware: Prozessoren
- Hardware: Netzteile
- Hardware: Speicher
- Hardware: Netzwerkschnittstellenkarten
- Hardware: PCI-Steckplätze
- Hardware: Remote-Zugriffskarte
- Speicher: Physische Datenträger
- Speicher: Virtuelle Datenträger
- Firmware
- Stromüberwachung
- Garantie

So zeigen Sie die Konfiguration und den Status der gesamten Datacenter-Hardware an:

1. Wählen Sie im **vSphere-Client** unter der Überschrift **Bestandsliste** die Option **Hosts und Cluster** aus.
2. Wählen Sie unter **Hosts und Cluster** ein Datacenter in der Baumstruktur aus und wählen Sie die Registerkarte **OpenManage Integration** aus.
3. Es wird eine Übersicht aller Hosts im Datacenter angezeigt. Suchen Sie in der Dropdown-Liste **Ansicht** eine Kategorie der Bestandsliste aus.
4. Geben Sie einen Filter für die Bestandslistendaten in das Textfeld **Filter** ein.
5. Klicken Sie auf **Aktualisieren**, um die angezeigte Bestandsliste zu aktualisieren.
6. Suchen Sie im Fenster **Speicherort für Download** nach einem Speicherort für die Bestandsliste und klicken Sie auf **Speichern**.

Verwalten von Verbindungsprofilen

Verbindungsprofile weisen einen Berechtigungsnachweis für den Zugriff und die Bereitstellung einer Reihe von Hostsystemen zu und enthalten typischerweise:

- Profilname und eindeutige Beschreibung (zur Unterstützung bei der Profilverwaltung)
- Eine Liste der Hosts, denen ein Verbindungsprofil zugewiesen wurde
- iDRAC-Berechtigungsnachweis
- Host-Anmeldeinformationen
- Erstellungsdatum
- Geändertes Datum
- Letzter geänderter Benutzer

Nach dem Ausführen des **Konfigurationsassistenten** erfolgt die Verwaltung von Anmeldedaten-Profilen von der Registerkarte OpenManage Integration for VMware vCenter **OpenManage Integration for VMware vCenter → Vorlagen und Profile**aus, unter Verwendung der folgenden Aktionen:

- Erstellen eines neuen Verbindungsprofils
- Anzeigen und Bearbeiten eines bestehenden Verbindungsprofils
- Löschen eines Verbindungsprofils
- Testen eines Verbindungsprofils
- Aktualisieren eines Verbindungsprofils

Anzeigen bzw. Bearbeiten eines vorhandenen Verbindungsprofils

Nachdem Sie ein Verbindungsprofil konfiguriert haben, können Sie den Verbindungsnamen, die Beschreibung, zugeordnete Hosts und der Berechtigungsnachweis für die iDRAC- und OMSA Agenten bearbeiten.
So zeigen Sie ein vorhandenes Verbindungsprofil an bzw. nehmen Änderungen daran vor:

1. Wählen Sie in der OpenManage Integration for VMware vCenter **Verbindungsprofile**.
2. Wählen Sie unter **Verfügbare Profile** das Profil aus, das Sie anzeigen bzw. bearbeiten möchten, und klicken Sie dann auf **Bearbeiten/Anzeigen**.
3. Geben Sie auf der Seite **Profilname und Beschreibung** den **Namen des Verbindungsprofils** und eine optionale **Beschreibung des Verbindungsprofils** ein, die dabei helfen, benutzerdefinierte Verbindungsprofile zu verwalten.
4. Wählen Sie auf der Seite **Zugewiesene Hosts** die Hosts für das Verbindungsprofil aus und klicken Sie auf **Weiter**.
5. Lesen Sie die Informationen auf der Seite **Anmeldeinformationen** und klicken Sie auf **Weiter**.
6. Auf der iDRAC-Seite, unter Anmeldeinformationen, führen Sie eine der folgenden Optionen aus:

   ANMERKUNG: Das iDRAC-Konto erfordert Administratorberechtigungen für die Aktualisierung der Firmware, Anwendung von Hardware-Profilen und die Bereitstellung des Hypervisors.

   - Für iDRACs, die für Active Directory, auf dem Sie Active Directory benutzen möchten, bereits konfiguriert und aktiviert sind, wählen Sie das Kontrollkästchen **Active Directory verwenden** aus; anderenfalls gehen Sie nach unten, um die iDRAC-Anmeldeinformationen zu konfigurieren.
     – Geben Sie im Textkästchen **Active Directory-Benutzername** den Benutzernamen ein. Geben Sie den Benutzernamen in einem dieser Formate ein: Domain\Benutzername oder Domain/Benutzername oder username@domain. Der Benutzername darf maximal 256 Zeichen enthalten. Weitere Informationen zu Benutzernamen-Einschränkungen finden Sie in der Dokumentation zu Microsoft Active Directory.
     – Geben Sie im Textfeld **Active Directory-Kennwort** das Kennwort ein. Das Kennwort darf maximal 127 Zeichen enthalten.
     – Geben Sie das Kennwort zur Bestätigung in das Textfeld **Kennwort bestätigen** ein.
     – Wählen Sie in der Zertifikatsprüfung-Drop-Down-Liste eine der folgenden Optionen aus:
       * Wählen Sie **Aktivieren** aus, um das iDRAC-Zertifikat herunterzuladen, zu speichern und für alle künftigen Verbindungen zu validieren.
       * Wählen Sie **Deaktivieren**, um keine Prüfung durchzuführen und das Zertifikat nicht zu speichern.
   - Um iDRAC-Anmeldeinformationen ohne Active Directory zu konfigurieren, führen Sie Folgendes aus:
     – Geben Sie im Textfeld **Benutzername** den Benutzernamen ein. Der Benutzername darf maximal 16 Zeichen enthalten. Weitere Informationen zur Benutzername-Einschränkungen für Ihre Version von iDRAC finden Sie in der iDRAC-Dokumentation.

       ANMERKUNG: Das lokale iDRAC-Konto erfordert Administratorberechtigungen für die Aktualisierung der Firmware, Anwendung von Hardware-Profilen und die Bereitstellung des Hypervisors.
     – Geben Sie im Textfeld **Kennwort** das Kennwort ein. Das Kennwort darf maximal 20 Zeichen enthalten.
     – Geben Sie das Kennwort zur Bestätigung in das Textfeld **Kennwort bestätigen** ein.
     – Wählen Sie in der Zertifikatsprüfung-Drop-Down-Liste eine der folgenden Optionen aus:
       * Wählen Sie **Aktivieren** aus, um das iDRAC-Zertifikat herunterzuladen, zu speichern und für alle künftigen Verbindungen zu validieren.
       * Wählen Sie **Deaktivieren**, um keine Prüfung durchzuführen und das iDRAC-Zertifikat nicht zu speichern.

7. Klicken Sie auf **Weiter**.
8. Auf der iDRAC-Seite, unter Host-Anmeldeinformationen, führen Sie eine der folgenden Optionen aus:

   - Für Hosts, die für Active Directory, auf dem Sie Active Directory benutzen möchten, bereits konfiguriert und aktiviert sind, wählen Sie das Kontrollkästchen **Active Directory verwenden** aus; anderenfalls gehen Sie nach unten, um Ihre Host-Anmeldeinformationen zu konfigurieren.

     – Geben Sie im Textkästchen **Active Directory-Benutzername** den Benutzernamen ein. Geben Sie den Benutzernamen in einem dieser Formate ein: Domain\Benutzername oder Domain/Benutzername oder username@domain. Der Benutzername darf maximal 256 Zeichen enthalten. Weitere Informationen zu Benutzernamen-Einschränkungen finden Sie in der Dokumentation zu Microsoft Active Directory.
     – Geben Sie im Textfeld **Active Directory-Kennwort** das Kennwort ein. Das Kennwort darf maximal 127 Zeichen enthalten.
     – Geben Sie das Kennwort zur Bestätigung in das Textfeld **Kennwort bestätigen** ein.
     – Wählen Sie in der Zertifikatsprüfung-Drop-Down-Liste eine der folgenden Optionen aus:

       * Wählen Sie **Aktivieren** aus, um das Host-Zertifikat herunterzuladen, zu speichern und für alle künftigen Verbindungen zu validieren.
       * Wählen Sie **Deaktivieren**, um keine Prüfung durchzuführen und das Host-Zertifikat nicht zu speichern.

   - Um Host-Anmeldeinformationen ohne Active Directory zu konfigurieren, führen Sie Folgendes aus:

     – Geben Sie den Benutzernamen in das Textfeld **Benutzername** ein. Der Benutzername muss „root“ sein.
     – Geben Sie im Textfeld **Kennwort** das Kennwort ein. Das Kennwort darf maximal 127 Zeichen enthalten.

       ANMERKUNG: Bei Servern, die nicht über eine iDRAC Express- oder iDRAC Enterprise-Karte verfügen, lautet das Ergebnis für den iDRAC-Verbindungstest „Für dieses System nicht anwendbar“.

       ANMERKUNG: Die OMSA-Anmeldeinformationen sind die gleichen, die auch für ESX- und ESXi-Hosts verwendet werden.

     – Geben Sie das Kennwort zur Bestätigung in das Textfeld **Kennwort bestätigen** ein.
     – Wählen Sie in der Zertifikatsprüfung-Drop-Down-Liste eine der folgenden Optionen aus:

       * Wählen Sie **Aktivieren** aus, um das Host-Zertifikat herunterzuladen, zu speichern und für alle künftigen Verbindungen zu validieren.
       * Wählen Sie **Deaktivieren**, um keine Prüfung durchzuführen und das Host-Zertifikat nicht zu speichern.

9. Klicken Sie auf **Speichern**.
10. Klicken Sie zum Schließen des Fensters auf das **X** in der rechten oberen Ecke.

Löschen eines Verbindungsprofils

Sie können ein Verbindungsprofil aus der Dell OpenManage Integration for VMware vCenter entfernen.
So löschen Sie ein Verbindungsprofil:

1. Klicken Sie in der **OpenManage Integration for VMware vCenter** auf **Verbindungsprofile**.
2. Wählen Sie unter **Verfügbare Profile** das zu löschende Profil aus und klicken Sie auf **Löschen**.
3. Klicken Sie in der folgenden Bestätigungsmeldung entweder auf **Löschen** oder auf **Abbrechen**.

Testen eines Verbindungsprofils

So testen Sie ein Verbindungsprofil:

1. Wählen Sie in der **OpenManage Integration for VMware vCenter Verbindungsprofile**.
2. Wählen Sie unter **Verfügbare Profile** das Verbindungsprofil aus und klicken Sie auf **Verbindung testen**, um den angegebenen iDRAC und die Host-Root-Anmeldeinformationen auf den ausgewählten Servern zu testen.
3. Verwenden Sie die Kontrollkästchen, um die Hosts auszuwählen, die Sie testen möchten, und klicken Sie dann auf **Ausgewählte testen**.
4. Klicken Sie zum Abbrechen aller ausgewählten Tests und des Testvorgangs auf **Alle Tests abbrechen**.
5. Klicken Sie zum Beenden auf **Fertig stellen**.

Aktualisieren eines Verbindungsprofils

So aktualisieren Sie ein Verbindungsprofil:

Klicken Sie auf **Aktualisieren**.

 **ANMERKUNG:** Wenn ein Host aus vCenter entfernt wird, wird es auch aus dem Verbindungsprofil gelöscht.

Systemereignisprotokolle in der Hostansicht im vSphere-Client

Das Systemereignisprotokoll stellt die Statusinformationen für die durch die OpenManage Integration for VMware vCenter ermittelte Hardware bereit.

Systemereignisprotokolle enthalten Informationen, die auf den folgenden Kriterien basieren:

Status	Es gibt verschiedene Status-Symbole: Informativ (blaues Ausrufezeichen), Warnung (gelbes Dreieck mit Ausrufezeichen), Fehler (rotes X).
Uhrzeit (Server-Uhrzeit)	Gibt die Uhrzeit und das Datum an, an dem das Ereignis aufgetreten ist.
Diese Seite durchsuchen	Zeigt die bestimmte Meldung, Servernamen, Konfigurationseinstellungen usw. an.

Die Schweregrade sind definiert als:

Info	Der Vorgang OpenManage Integration for VMware vCenter wurde erfolgreich abgeschlossen.
Warnung	Der Vorgang OpenManage Integration for VMware vCenter ist teilweise fehlgeschlagen und wurde teilweise erfolgreich abgeschlossen.
Fehler	Der Vorgang OpenManage Integration for VMware vCenter ist fehlgeschlagen.
Sicherheit	Enthält Informationen zur Systemsicherheit.

Sie können das Protokoll in einer externen csv-Datei speichern.

Weitere Informationen:

- Anzeigen der Systemereignisprotokolle für einen bestimmten Host

Anzeigen von Protokollen im Dell Management Center

Dell Management Center-Protokolle enthalten Statusinformationen für die erfasste Hardware und eine Aufzeichnung der Benutzeraktionen.

So zeigen Sie Protokolle im Dell Management Center an:

1. Klicken Sie im linken Fensterbereich von **Dell Management Center** auf **Protokoll**.
2. Klicken Sie zum Aktualisieren des Protokolls mit den neuesten Daten auf **Aktualisieren**.
3. Klicken Sie zum Auswählen einer Kategorie für den Schweregrad als Filter für die Protokolldaten in der Dropdown-Liste **Alle Kategorien** auf eine der folgenden Kategorien: „Alle Kategorien", „Info", „Warnung", „Fehler" oder „Sicherheit".
4. Klicken Sie zum Auswählen eines Datumbereichs als Filtern für die Protokolldaten in der Dropdown-Liste **Last Week** auf eine der folgenden Optionen: „Letzte Woche", „Letzter Monat", „Letztes Jahr" oder „Benutzerdefinierter Bereich".

   Wenn Sie die Option „Benutzerdefinierte Bereich" auswählen, werden die Dropdown-Listen **Anfangsdatum Enddatum** angezeigt.
5. Wenn Sie den benutzerdefinierten Datumsbereich ausgewählt haben:
   a. Klicken Sie auf den Kalender, um das **Startdatum** auszuwählen.
   b. Klicken Sie auf den Kalender, um das **Enddatum** auszuwählen.
   c. Klicken Sie zum Speichern Ihrer Konfiguration auf **Übernehmen**.
6. Legen Sie fest, wie das Protokoll angezeigt wird. Dazu verwenden Sie die Anzeige-Bedienelemente, um die **Datensätze pro Fenster** festzulegen, zu einer bestimmten **Seite** zu wechseln, oder um vorwärts oder rückwärts zu blättern.
7. Klicken Sie zum Exportieren des Protokollinhalts in eine csv-Datei auf **Exportieren**.
8. Suchen Sie im Fenster „Speicherort für Download" nach einem Speicherort für das Protokoll und klicken Sie auf **Speichern**.

Anzeigen der Ereignisprotokolle für einen bestimmten Host

Systemhardware-Ereignisprotokolle enthalten Informationen, die auf den folgenden Kriterien basieren:

- Status

  Es gibt verschiedene Status-Symbole: Informativ (blaues Ausrufezeichen), Warnung (gelbes Dreieck mit Ausrufezeichen), Fehler (rotes X).
- Uhrzeit (Server-Uhrzeit)

  Zeigt die Uhrzeit und das Datum an, an dem das Ereignis aufgetreten ist.
- Diese Seite durchsuchen

  Zeigt die bestimmte Meldung, Servernamen, Konfigurationseinstellungen usw. an.

So zeigen Sie das Systemereignisprotokoll für einen bestimmten Host an:

1. Wählen Sie im **vSphere-Client** unter der Überschrift **Bestandsliste** die Option **Hosts und Cluster** aus.
2. Wählen Sie in der Strukturansicht das Hostsystem aus.
3. Wählen Sie die Registerkarte **OpenManage Integration** aus.
4. Klicken Sie unter **Letzte Systemprotokolleinträge** zum Anzeigen des Fensters **Systemereignisprotokoll** auf **Details**.
5. Klicken Sie zum Aktualisieren des **Systemereignisprotokolls** auf **Protokoll aktualisieren**.
6. Wählen Sie eine der folgenden Optionen, um die Anzahl der Ereignisprotokolleinträge zu beschränken (filtern):

   - Geben Sie einen Text in das Textfeld für den Suchfilter ein, um die Protokolleinträge dynamisch zu filtern.
   - Klicken Sie zum Leeren des Textfeldes für den Filter auf das **X**. Es werden wieder alle Ereignisprotokolleinträge angezeigt.
7. Klicken Sie zum Löschen aller Ereignisprotokolleinträge auf **Protokoll löschen**. Es wird eine Meldung angezeigt, dass alle Protokolleintäge nach dem Leeren der Liste gelöscht werden. Wählen Sie eine der folgenden Optionen aus:

- Klicken Sie zum Löschen der Protokolleinträge auf **OK**.
- Klicken Sie zum Abbrechen des Vorgangs auf **Abbrechen**.

8. Klicken Sie zum Exportieren des Ereignisprotokolls in eine csv-Datei auf **Export**.
9. Suchen Sie nach einem Speicherort für das Systemereignisprotokoll und klicken Sie auf **Speichern**.

Allgemeines zu Firmware-Aktualisierungen

Der Standort, auf dem Server Firmware-Aktualisierungen erhalten, ist eine globale Einstellung, die in der OpenManage Integration for VMware vCenter im Register „Einstellungen" verfügbar ist.

Die Einstellungen für das Firmware-Repository enthalten den Speicherort des Firmware-Katalogs, der zum Aktualisieren von bereitgestellten Servern verwendet wird. Es gibt zwei Arten von Speicherorten:

Dell (ftp.dell.com)	Verwendet das Repository zur Firmware-Aktualisierung von Dell (**ftp.dell.com**). OpenManage Integration for VMware vCenterr lädt die ausgewählten Firmware-Aktualisierungen von Dell herunter.
Freigegebene Netzwerkordner	Erstellt mit Dell Repository Manager™. Diese lokalen Repositorien befinden sich auf der CIFS- oder der NFS-Dateifreigabe.



ANMERKUNG: Nachdem ein Repository erstellt wurde, speichern Sie es an einem Speicherort, auf den registrierte Hosts zugreifen können. Die Kennwörter für Repositorien dürfen nicht mehr als 31 Zeichen umfassen. Folgende Zeichen dürfen dabei nicht verwendet werden: @, &, %, ', ", ,(Komma), < >

Der Assistent zur Aktualisierung der Firmware prüft stets die erforderlichen Mindest-Firmware-Versionen für iDRAC, BIOS und den Lifecycle Controller und versucht, diese auf die erforderlichen Mindestversionen zu aktualisieren. Wenn die iDRAC-, Lifecycle- und BIOS-Firmware-Versionen die Mindestanforderungen erfüllen, ermöglicht der Assistent zur Aktualisierung der Firmware alle Firmware-Aktualisierungen, einschließlich iDRAC, Lifecycle Controller, RAID, NIC/LOM, Netzteile, BIOS usw.



ANMERKUNG: Bei Servern der 9. und 10. Generation können die BIOS/BMC/DRAC-Firmware-Versionen nur auf der „Cluster View"-Ebene in vCenter oder auf der Seite „Übersicht" in der individuellen Hostansicht angezeigt werden. Die Informationen zur Firmware-Version sind in der individuellen Hostansicht unter „Firmware" nicht aktiv und remote Firmware-Aktualisierungen stehen nicht zur Verfügung.

Firmware-Versionen nach dem 14. Oktober 2010

Bei Firmware, die am oder nach dem 14. Oktober 2010 aktualisiert wurde, wird der Assistent zur Aktualisierung der Firmware ausgeführt.

Firmware-Versionen neuer als 29. Juli 2009 und vor dem 14. Okober 2010

Wenn Ihre Firmware am oder nach dem 29. Juli 2009 und vor dem 14. Oktober 2010 aktualisiert wurde, wird der Assistent zur Aktualisierung der Firmware nicht angezeigt, stattdessen erhalten Sie ein ISO-Paket zur Aktualisierung Ihrer Firmware. Auch nach dieser Aktualisierung verfügen Sie eventuell noch nicht über die aktuellste Firmware. Wir empfehlen, dass Sie nach der Installation des Pakets den Assistenten zur Aktualisierung der Firmware erneut ausführen.

Firmware-Versionen vor 29. Juli 2009

Wenn Ihre Firmware älter als 29. Juli 2009 ist, müssen Sie die ISO-Datei herunterladen und ausführen, um Ihre Maschinen zu aktualisieren. Wir empfehlen, dass Sie nach der Installation des Pakets den Assistenten zur Aktualisierung der Firmware erneut ausführen.

Weitere Informationen:

- Einrichten des Firmware-Repositorys

Ausführen des Assistenten zum Aktualisieren der Firmware

Diese Funktionalität steht nur für die Dell-Server der 11. Generation und später zur Verfügung, die entweder eine iDRAC Express- oder eine iDRAC-Enterprise-Karte haben. Falls Ihre Firmware am oder nach dem 14. Oktober 2010 installiert wurde, können Sie Ihre Firmwareversion automatisch mit dem Assistenten zur Firmwareaktualisierung aktualisieren.



ANMERKUNG: Ändern Sie zum Schutz gegen Fehler durch Zeitüberschreitung des Browsers die Standardzeit auf 30 Sekunden. Weitere Informationen zum Ändern der Standardzeitüberschreitungseinstellungen finden Sie unter „Warum wird eine Fehlermeldung nachdem ich auf den Firmware-Aktualisierungslink geklickt habe, angezeigt?" im Abschnitt „Fehlerbehebung" im *Benutzerhandbuch*.



ANMERKUNG: Mit einer Demo-/Test-Lizenz können Sie den Firmware-Assistenten für die Dauer Ihrer Lizenz verwenden.

So führen Sie den Firmware-Update-Assistenten aus:

1. Klicken Sie in **vSphere-Client** → **Registerkarte „OpenManage Integration"** → **Host-Informationen** auf **Firmware** → **Firmware-Update-Assistent ausführen.**
2. So verwenden Sie die Option **Eine einzelne Firmwareaktualisierung von einer Datei laden**:
   a. Geben Sie den Dateipfad in folgendem Format ein:

      ```
      CIFS: \\<host accessible share path>\<FileName>.exe or NFS: host:/share/
      filename.exe
      ```

   b. Falls Sie NFS haben, gehen Sie zu Schritt 7 weiter. Andernfalls geben Sie den **Benutzernamen** und das **Kennwort** in einem Domänenformat ein, das Zugriff auf das gemeinsame Laufwerk hat.
   c. Fahren Sie mit Schritt 7 fort.

   Als Alternative verwenden Sie die Option **Vom Repository aus aktualisieren**:

   a. Wählen Sie **Vom Repository aus aktualisieren**.
   b. Stellen Sie sicher, dass Sie eine Netzwerkverbindung zu **ftp.dell.com** haben.
   c. Klicken Sie auf **Weiter**.
3. Wählen Sie das Bündel für Ihren Host aus und klicken Sie auf **Weiter**.
4. Wählen Sie die gewünschten Firmwareaktualisierungen aus und klicken Sie auf **Weiter**. Komponenten, die zurückgestuft wurden, bereits aktuell sind oder für die derzeit eine Aktualisierung geplant ist, können nicht ausgewählt werden. Falls Sie das Kontrollkästchen **Zurückstufung der Komponenten gestatten** markieren, wählen Sie die Optionen aus, die als Zurückstufung aufgeführt sind. Die Auswahl dieser Option ist nur fortgeschrittenen Benutzern empfohlen, die die Folgen einer Zurückstufung der Firmware verstehen.
5. Wählen Sie die gewünschte Option zum Neustart aus.

   - **Gehen Sie in den Wartungsmodus über, wenden Sie die Aktualisierungen an und führen Sie dann einen Neustart durch.**

     Der Host tritt in den Wartungsmodus über. Falls der Host nicht in den Wartungsmodus übertreten kann, wird der Host nicht neu gestartet, und die Aktualisierung wird während des nächsten Neustarts angewandt. Markieren Sie das Kontrollkästchen **Wartungsmodus verlassen, wenn die Firmwareaktualisierung beendet ist,** um den Wartungsmodus nach der Aktualisierung zu verlassen.
   - **Wenden Sie die Aktualisierungen beim nächsten Neustart an.**

     Um eine Dienstunterbrechung zu vermeiden, wird empfohlen, dass der Host vor dem Neustart in den Wartungsmodus übergeht.
   - **Aktualisierungen anwenden und den Neustart erzwingen, ohne in den Wartungsmodus überzugehen.**

     Die Aktualisierung wird angewandt, und ein Neustart wird ausgeführt, auch wenn der Host nicht im Wartungsmodus ist. Diese Methode ist nicht empfehlenswert.

6. Klicken Sie auf **Fertigstellen**.
7. Um zu überprüfen, ob die Aktualisierung erfolgreich war, wählen Sie im Dell Management Center **Job-Warteschlange** → **Bestandsaufnahmenverlauf** → **Jetzt ausführen**, und um die neuen Versionen zu sehen, wechseln Sie in **vSphere-Client** → **Registerkarte „OpenManage Integration“** und klicken Sie auf **Firmware**.

Aktualisieren älterer Firmware-Versionen

Die Firmware muss eine Mindestversion aufweisen, damit der Assistent zur Firmware-Aktualisierung ausgeführt werden kann. Anderenfalls werden Optionen angezeigt, die Ihnen dabei helfen, Ihre Firmware so zu aktualisieren, dass der Assistent zur Firmware-Aktualisierung ausgeführt werden kann. In der Regel ist es für Firmware vor dem 29. Juli 2009 erforderlich, dass Sie eine ISO-Datei herunterladen und installieren. Lesen Sie dazu Firmware-Aktualisierungen. Bei Firmware, die zwischen dem 29. Juli 2009 und dem 14. Oktober 2010 installiert wurde, können Sie ein ISO-Paket wählen, das automatisch vom OpenManage Integration for VMware vCenter installiert wird. Firmware, die nach dem 14. Oktober 2010 aktualisiert wurde, kann den Assistenten zur Firmware-Aktualisierung ausführen. Firmware-Aktualisierungen werden vom vSphere-Client auf der Registerkarte „OpenManage Integration“ des Hosts ausgeführt. Weitere Informationen zum Einrichten des Repositorys finden Sie unter Einrichten des Firmware-Repositorys.
So aktualisieren Sie ältere Firmware-Versionen:

1. Klicken Sie im **vSphere-Client** auf der Registerkarte **OpenManage Integration** unter **Hostaktionen** auf **Assistent zur Firmware-Aktualisierung ausführend**.

   Das Dialogfeld „Aktualisierung erforderlich“ wird angezeigt, wenn Ihr Host eine Firmwareversion ausführt, die nicht mehr vom Assistenten unterstützt wird. In diesem Fall werden Sie aufgefordert, eine ISO-Datei herunterzuladen und auszuführen, oder Sie erhalten ein Aktualisierungspaket, das Sie zunächst ausführen müssen.
2. Führen Sie eine der folgenden Möglichkeiten im Dialogfeld **Aktualisierung erforderlich** aus:
   - Aktivieren Sie das Kontrollkästchen **Exit maintenance mode after firmware update completes** (Wartungsmodus nach Abschluss der Firmware-Aktualisierung beenden), um den Wartungsmodus nach der Firmware-Aktualisierung automatisch zu beenden.
   - Lassen Sie das Kontrollkästchen deaktiviert, um den Wartungsmodus aufzurufen, in dem Sie den Rechner prüfen bzw. testen können, bevor Sie ihn wieder dem Cluster hinzufügen.
3. Klicken Sie auf **Aktualisieren**.
4. Das Dialogfeld **Erfolg** zeigt Ihnen an, ob momentan eine Aktualisierung ausgeführt wird.

   Wenn Sie das Kontrollkästchen **Verlassen Sie den Wartungsmodus nach Beenden der Firmwareaktualisierung** aktiviert haben, versetzt die Firmware den Host in den Wartungsmodus und bootet dann automatisch neu. Anderenfalls bleibt der Host im Wartungsmodus.
5. Achten Sie auf den Bereich **Zuletzt ausgeführte Tasks** im vSphere-Client, um den Aktualisierungsprozess zu überwachen.

   Nach diesem Vorgang führen Sie den Assistenten zur Firmware-Aktualisierung erneut aus, um sicherzustellen, dass Ihre Firmware vollständig aktualisiert wurde.

Ausführen des Assistenten zum Aktualisieren der Firmware für Cluster und Datazentren

Diese Funktionalität steht nur für Dell-Servern der 11.Generation oder später, die entweder eine iDRAC Express- oder eine iDRAC-Enterprise-Karte haben, zur Verfügung. Falls Ihre Firmware am oder nach dem 14. Oktober 2010 installiert wurde, können Sie Ihre Firmwareversion automatisch mit dem Firmware-Update-Assistenten aktualisieren. Dieser Assistent aktualisiert nur Hosts, die Teil eines Verbindungsprofils und in Bezug auf Firmware, CSIOR-Status, Hypervisor und OMSA-Status (nur Server der 11. Generation) konform sind. Sollte Ihr Host nicht aufgeführt sein, führen Sie den Übereinstimmungs-Assistenten für vSphere Hosts im OpenManage Integration for VMware vCenter aus oder wählen Sie den nicht aufgeführten Host in der Ansicht „Hosts und Cluster“ aus und verwenden Sie den Assistenten zur Aktualisierung der Firmware. Typischerweise dauert eine Aktualisierung der Firmware-Komponenten für jeden Host 30-60 Minuten. Aktivieren Sie DRS auf einem Cluster, sodass die virtuellen Maschinen migriert werden können, wenn ein Host während des Firmware-Aktualisierungsprozesses in den Wartungsmodus ein- oder austritt. Sie können nur einen Firmware-Aktualisierungs-Task gleichzeitig planen oder ausführen.

Verwenden Sie zum Export aus dem Assistenten die CSV-Taste. Die Suche steht für das Lokalisieren eines bestimmten Clusters, Datenzetrums, Host oder jeden Themenpunkt der Datentabelle außer für „Datum der Anwendung“ zur Verfügung.

 **ANMERKUNG:** Aktualisieren Sie die Firmware immer zusammen als Teil des Repository-Pakets: BIOS, iDRAC und Lifecycle Controller.

 **ANMERKUNG:** Weitere Informationen zum Ändern der Standardzeitübschreitungseinstellungen finden Sie unter „Warum wird eine Fehlermeldung, nachdem ich auf den Firmware-Aktualisierungslink geklickt habe, angezeigt?“ im Abschnitt „Fehlerbehebung“ im *Benutzerhandbuch*.

Sie können den Status der Firmware-Aktualisierungs-Jobs auf der Seite „Job-Warteschlange“ anzeigen und verwalten. Siehe Anzeige von Firmware-Aktualisierungen für Cluster und Datenzentren.

1. Wählen Sie im **vSphere-Client** unter der Überschrift **Bestandsaufnahme** die Option **Hosts und Cluster** aus.
2. Wählen Sie in der Strukturansicht unter **Hosts und Cluster** ein Datenzentrum oder Cluster aus und wählen Sie dann die Registerkarte **OpenManage Integration.**
3. Klicken Sie auf **Firmware aktualisieren**.

   Sollte dieser Link nicht aktiviert sein oder sollten Sie eine Pop-up-Meldung beim Klicken auf diese Option erhalten, wird bereits ein Firmware-Aktualisierungs-Job ausgeführt oder es wurde einer geplant. Schliessen Sie das Dialogfeld, warten Sie und versuchen Sie den Vorgang später erneut. Sehen Sie sich den Status aller Jobs auf der Registerkarte „Firmware-Aktualisierungs-Jobs“ in der Job-Warteschlange an.
4. Lesen Sie die Informationen über die Aktualisierung auf der Startseite, bevor Sie mit dem Assistenten fortfahren.
5. Klicken Sie auf **Weiter**.
6. Überprüfen Sie auf der Seite „Firmware-Bestandsaufnahme“, welche Komponenten bereits auf den Systemen installiert sind.
7. Klicken Sie auf **Weiter**.
8. Wählen Sie auf der Seite „Aktualisierungs-Pakete“ mithilfe der Kontrollkästchen die Aktualisierungs-Pakete.
9. Klicken Sie auf **Weiter**.
10. Wählen Sie auf der Seite „Zu aktualisierende Systeme/Komponenten“ mithilfe der Kontrollkästchen die zu aktualisierenden oder zurückzustufenden Komponenten aus. Möchten Sie zurückstufen, wählen Sie das Kontrollkästchen **Erlauben des Zurückstufens der Komponenten**.

     **ANMERKUNG:** Wenn Sie alle Komponenten ausgewählt haben, aber dennoch einige nicht markiert sind, bedeutet das, dass für diese Komponenten keine Aktualisierungen zur Verfügung stehen. Diese Komponenten können nur für eine Zurückstufung ausgewählt werden.
11. Klicken Sie auf **Weiter**.
12. Überprüfen Sie auf der Seite „Firmware-Aktualisierungs-Informationen“ die Komponenten, die Sie für eine Aktualisierung oder Zurückstufung ausgewählt haben.
13. Klicken Sie auf **Weiter**.
14. Führen Sie die folgenden Schritte auf der Seite „Geplante Firmware-Aktualisierungen“ unter „Jobname“ aus:
    a. Im Textfeld „Firmware-Aktualisierungs-Jobname“ geben Sie den **Firmware-Aktualisierungs-Jobnamen** ein.

       Dies ist ein Pflichtfeld. Ist das Feld nicht ausgefüllt, wird die Aktualisierung nicht geplant. Verwenden Sie keinen bereits vorhandenen Namen. Sollten Sie den Namen gesäubert haben, kann er wieder verwendet werden.

    b. Geben Sie in der Firmware-Aktualisierungsbeschreibung eine **Beschreibung** ein.
15. Führen Sie einen der folgenden Schritte unter „Job-Zeitplan“ aus:

    ANMERKUNG: Die Auswahl einer Option ist obligatorisch. Sollte keine Option ausgewählt werden, wird die Aktualisierung blockiert.

    - Wenn Sie den Aktualisierungs-Job sofort ausführen möchten, klicken Sie auf **Jetzt aktualisieren** und dann auf **Fertigstellen**.

- Möchten Sie den Aktualisierungs-Job später ausführen, klicken Sie auf **Aktualisierung planen** und führen die folgenden Schritte aus:

    1. Im Kontrollkästchen „Kalender“ wählen Sie den **Monat und Tag** aus.
    2. Im Textfeld „Zeit“ geben Sie die **Uhrzeit** in SS:MM ein und klicken auf **Fertigstellen**.

    ANMERKUNG: Die Uhrzeit entspricht der lokalen Zeitzone des physischen Standorts Ihres Clients. Ungültige Eingaben von Zeitwerten resultieren in einer blockierten Aktualisierung.

Anzeige des Firmware-Aktualisierungs-Status für Cluster und Datenzentren

Zum Anzeigen von Informationen auf dieser Seite, führen Sie eine Firmware-Aktualisierung für ein Cluster oder ein Datenzentrum aus. Diese Seite zeigt nur Informationen über Firmware-Aktualisierungen von Clustern und Datenzentren an. Siehe Ausführen des Assistenten zum Aktualisieren der Firmware für Cluster und Datenzentren.
Auf dieser Seite können Sie Firmware-Aktualisierungs-Jobs aktualisieren, säubern oder abbrechen.

1. Wählen Sie im Dell Management Center **Job-Warteschlange** → **Firmware-Aktualisierungs-Jobs** aus.
2. Zum Anzeigen der aktuellsten Informationen klicken Sie auf **Aktualisieren**.
3. Anzeige des Status in der Datentabelle. Dieses Raster enthält die folgenden Informationen über Firmware-Aktualisierungs-Jobs:

    - Status
    - Geplante Zeit
    - Name
    - Beschreibung
    - Erfassungsgröße

      Die Erfassungsgröße ist die Anzahl der Server auf diesem Firmware-Bestandsaufnahme-Job.
    - Fortschrittszusammenfassung

      Die Fortschrittszusammenfassung listet die Fortschrittsdetails dieser Firmware-Aktualisierung auf.
4. Um mehr Details zu einem bestimmten Job in der Datentabelle anzuzeigen, klicken Sie auf **Details**.

    Hier finden Sie die folgenden Details:

    - Service-Tag-Nummer
    - iDRAC IP (iDRAC-IP)
    - Status
    - Warnungen
    - Firmware-Aktualisierungs-Job-Details
    - Startzeit
    - Ende um
5. Wenn Sie eine geplante Firmware-Aktualisierung, die nicht ausgeführt wird, in derselben Reihe, wie den abzubrechenden Job abbrechen, klicken Sie auf **Abbrechen**.
6. Wenn Sie die geplanten Firmware-Aktualisierungen säubern möchten, klicken Sie auf **Job-Warteschlange säubern**.

    Sie können nur Jobs säubern die beendet oder geplant sind.
7. Wählen Sie **Älter als Datum und Job-Status** aus und klicken Sie auf **Anwenden**. Die ausgewählten Jobs werden aus der Warteschlange entfernt.

Erweiterte Hostverwaltung mit vCenter

Die erweiterten Tasks zur Hostverwaltung sind Hostsystem-basierte Maßnahmen, mit denen ein Administrator einen physischen Server in der Datacenter-Umgebung identifizieren, Server-basierte Verwaltungsaufgaben starten und

Informationen zur Servergarantie anzeigen kann. Alle diesen Maßnahmen werden entweder auf der Registerkarte „OpenManage Integration“ in vCenter oder durch Klicken mit der rechten Maustaste auf den Host in der Ansicht *Hosts und Cluster* für ein bestimmtes Hostsystem aufgerufen.

Einrichten einer Anzeige an der Frontblende eines physischen Servers

Sie können ein Anzeigelicht an der Frontblende eines physischen Servers in einer großen Datacenter-Umgebung über einen bestimmten Zeitraum blinken lassen, so dass Sie den Server leichter erkennen können.
So richten Sie die Anzeigeleuchte an der Frontblende eines physischen Servers ein:

1. Wählen Sie im **vSphere-Client** unter der Überschrift **Bestandsaufnahme** die Option **Hosts und Cluster** aus.
2. Wählen Sie unter **Hosts und Cluster** das Hostsystem in der Baumstruktur aus und klicken Sie auf die Registerkarte **OpenManage Integration**.
3. Wählen Sie unter **Hostaktionen** die Option **Blinkanzeigelicht**.
4. Wählen Sie eine der folgenden Optionen:
    - Klicken Sie zum Einschalten des Blinkens und zum Einrichten einer Dauer im Dialogfeld **Anzeigelicht** auf **Blinken eingeschaltet**, und wählen Sie in der Dropdown-Liste „Zeitüberschreitung“ eine Dauer aus, dann klicken Sie auf **OK**.
    - Klicken Sie zum Ausschalten des Blinkens im Dialogfeld **Anzeigelicht** auf **Blinken ausgeschaltet** und dann auf **OK**.

Server-basierte Verwaltungstools

Es gibt zwei Server-basierte Verwaltungstools, iDRAC (Integrated Dell Remote Access Controller) und OMSA (OpenManage Server Administrator), die beide von der Registerkarte **vSphere Client → OpenManage Integration** gestartet werden. Über den Verwaltungskonsole-Link im linken Fensterbereich haben Sie Zugriff auf:

- Remotezugriff starten.

  Verwenden Sie diese Option, um die iDRAC-Benutzeroberfläche zu starten
- OMSA starten

  Verwenden Sie diese Option, um die Internetadresse der OpenManage Server Administrator-Benutzeroberfläche aufzurufen, die entweder im Konfigurationsassistenten oder über **Einstellungen → Allgemein**eingegeben wurde. Sie müssen die URL für den Server Administrator-Webserver auf einer Windows-basierten Managementstation installieren.
- Wenn Sie ein Blade-System verwenden, starten Sie den CMC, um die Benutzeroberfläche des Chassis Management Controller zu starten. Wenn Sie kein Blade-System verwenden, wird dies nicht angezeigt.

Garantieabfrage

Die Garantieabfrage bietet die folgenden Informationen zu Dell-Servern:

- Aktualisierte Servicegarantie-Informationen durch Übertragen der Service-Tag-Nummer des Hosts
- Garantieinformationen, die in festgelegten Intervallen aktualisiert werden
- Sichere Übertragung dank Proxyserver und Berechtigungsnachweis

 **ANMERKUNG:** Dell speichert keine übertragenen Service-Tag-Informationen.

Verwandte Aufgaben:

- Ausführen eines Garantieabfrage-Jobs
- Anzeigen der Servergarantie-Informationen für einen einzelnen Host

- Anzeigen der Garantieinformationen für ein gesamtes Datacenter

Anzeigen der Servergarantie-Informationen für ein gesamtes Datacenter

Nachdem die Garantieabfrage-Aufgabe abgeschlossen wurde, können Sie die Servergarantie-Informationen im vSphere-Client auf der Seite „Datencenter-Ansicht" anzeigen.

So zeigen Sie die Servergarantie-Informationen für ein gesamtes Datacenter an:

1. Klicken Sie im vSphere-Client unter der Überschrift **Bestandsaufnahme** auf die Option **Hosts und Cluster**.
2. Wählen Sie unter **Hosts und Cluster** ein Datacenter in der Baumstruktur aus und klicken Sie auf die Registerkarte **OpenManage Integration**.
3. Es wird eine Übersicht aller Hosts im Datacenter angezeigt. Wählen Sie in der Dropdown-Liste „Ansicht" die Option **Garantie** aus.
4. Geben Sie einen Filter für die Garantiedaten in das Textfeld **Filter** ein.
5. Klicken Sie zum Aktualisieren der angezeigten Bestandsaufnahme auf **Aktualisieren**.
6. Klicken Sie zum Exportieren der Bestandsaufnahme als eine csv-Datei auf **Exportieren**. Suchen Sie im Fenster „Speicherort für Download" nach einem Verzeichnis, in dem die Bestandsaufnahme gespeichert werden soll, und klicken Sie auf **Speichern**.

Anzeigen der Servergarantie-Informationen für einen einzelnen Host

Nachdem der Garantieabfrage-Job abgeschlossen wurde, können Sie die Garantieinformationen für einen einzelnen Host im vSphere-Client auf der Seite „Host View" (Hostansicht) anzeigen.

So zeigen Sie die Servergarantie-Informationen für einen einzelnen Host an:

1. Klicken Sie im vSphere-Client unter der Überschrift **Bestandsaufnahme** auf die Option **Hosts und Cluster**.
2. Wählen Sie unter **Hosts und Cluster** das Hostsystem in der Baumstruktur aus und klicken Sie auf die Registerkarte **OpenManage Integration**.
3. Klicken Sie zum Anzeigen der Systemgarantie-Informationen auf **Garantie**. Die Informationen auf der Seite „Garantiestatus" umfassen Folgendes:

   - Anbieter und Beschreibung der Garantie
   - Start- und Enddaten sowie Restlaufzeit der Garantie in Tagen
   - Status der Garantie (aktiv, inaktiv) und Datum, wann die Garantieinformationen das letzte Mal aktualisiert wurden

5

Hardware-Management

Voraussetzungen:

Für eine erfolgreiche Hardware-Einrichtung und -Bereitstellung müssen die physischen Server im Bereitstellungsassistenten angezeigt werden. Alle physischen Server müssen die folgenden Voraussetzungen erfüllen:

- Informationen zu den bestimmten Hardware-Support-Informationen finden Sie in *OpenManage Integration for VMware vCenter Versionshinweise*.
- Der Server muss die folgenden unterstützten Mindestversionen von iDRAC-Firmware, Lifecycle-Controller und BIOS aufweisen. Informationen zu den bestimmten Hardware-Support-Informationen finden Sie in *OpenManage Integration for VMware vCenter Versionshinweise*.

   ANMERKUNG: Wenn die Firmware-Versionen veraltet sind, ist eventuell ein zweistufiger Prozess zur Aktualisierung der Firmware erforderlich. Ausführliche Informationen zur Aktualisierung finden Sie in der Firmware-Dokumentation.

- Das OpenManage Integration for VMware vCenter unterstützt die Bereitstellung nur mit eingebetteten/integrierten LOMs. Sie können die NICs in den PCI-Steckplätzen manuell nach der Bereitstellung konfigurieren. Wenn Sie NIC-Zusatzadapter verwenden, müssen auf dem System Host-LOMs aktiviert sein.
- Das OpenManage Integration for VMware vCenter ermöglicht die Bereitstellung auf einem internen Dual SD-Modul (nur Hypervisor) oder auf lokalen Festplatten. Das interne Dual SD-Modul muss vom BIOS aktiviert werden, bevor Sie den Hypervisor mit dem OpenManage Integration for VMware vCenter bereitstellen können. Sie können die Verwaltung von Netzwerkschnittstellenkarten manuell ändern und das System zum vCenter hinzufügen.

  ANMERKUNG: Informationen zu den unterstützten Dual-SD-Modulen finden Sie in der jeweiligen Server-Produktdokumentation.

- Wenn der iDRAC im dedizierten Modus konfiguriert ist, müssen dessen Netzwerkschnittstellenkarten aktiviert werden, um mit dem OpenManage Integration for VMware vCenter kommunizieren zu können.
- CSIOR muss aktiviert sein. Darüber hinaus müssen Sie vor dem Initiieren von Auto Discovery sicherstellen, dass die abgerufenen Daten aktuell sind und das System muss vollständig aus und dann wieder eingeschaltet werden.
- Dell-Server können mit Auto Discovery bestellt und die Handshaking-Optionen werksseitig vorkonfiguriert werden. Ist ein Server nicht mit diesen Optionen vorkonfiguriert, müssen Sie die IP-Adresse des OpenManage Integration for VMware vCenter manuell eingeben oder ihr lokales Netzwerk konfigurieren, um diese Informationen bereitzustellen.
- Wenn das OpenManage Integration for VMware vCenter nicht für die Hardwarekonfiguration verwendet wird, müssen Sie vor einer Hypervisor-Bereitstellung sicherstellen, dass die folgenden Bedingungen erfüllt sind:
  - Aktivieren Sie das VT (Virtualization Technology)-Flag im BIOS.
  - Stellen Sie die Bootreihenfolge des Systems entweder auf eine bootfähige virtuelle Festplatte oder ein internes Dual SD-Modul für die Installation des Betriebssystems ein.
- Wenn das OpenManage Integration for VMware vCenter für die Hardwarekonfiguration verwendet wird, ist die BIOS-Einstellung für VT automatisch aktiviert, auch wenn die BIOS-Konfiguration kein Teil des Hardwareprofils ist. Die Express/Clone RAID-Konfiguration ist erforderlich, wenn keine virtuelle Festplatte auf dem Zielsystem vorhanden ist.
- Weisen Ihre Server Versionen vor Dell PowerEdge-Servern der12. Generation auf, installiert der Bereitstellungsprozess das OpenManage Server Administrator-Paket auf dem Zielsystem und konfiguriert das SNMP-Trap-Ziel automatisch so, dass es auf das OpenManage Integration for VMware vCenter verweist.
- Für die Bereitstellung werden benutzerdefinierte ESXi-Images benötigt, die *alle* Dell-Treiber enthalten. Auf der Dell-Seite „Treiber und Downloads“ finden Sie die korrekten Images. Speichern Sie diese benutzerdefinierten Images auf einen Speicherort, auf den Sie während der Bereitstellung zugreifen können. Eine aktuelle Liste mit allen unterstützten ESXi-Versionen für diese Version finden Sie in den Versionshinweisen.

- *OpenManage Integration for VMware vCenter* unterstützt BIOS-Modus nur um automatisch einen Hypervisor auf dem Zielserver bereitzustellen. Stellen Sie sicher, dass Sie im Refernz-Hardware-Profil BIOS-Modus vor dem Anwenden des Hypervisor-Profils ausgewählt haben. Falls kein Hardware-Profil ausgewählt wurde, stellen Sie sicher, dass Sie den Startmodus manuell als BIOS konfigurieren und starten Sie den Server neu, bevor Sie das Hypervisor-Profil anwenden.



ANMERKUNG: Betriebssystembereitstellung von OpenManage Integration for VMware vCenter (OMIVV) schlägt fehl, wenn der Boot-Modus auf dem Ziel-Computer auf UEFI gesetzt ist

Einrichtung – Übersicht

Nachdem eine Bestandsliste der physischen Komponenten in einem Datacenter fertig gestellt wurde, stehen alle automatisch ermittelten Bare-Metal-Systeme dem OpenManage Integration for VMware vCenter für die Zero-Touch-Hardewareeinrichtung und die Hypervisor-Bereitstellung zur Verfügung. Für die Vorbereitung dieser Systeme zur Einrichtung und Bereitstellung müssen Sie Folgendes ausführen:

Erstellen eines Hardwareprofils — Enthält die Hardwareeinstellungen, die von einem Referenzserver gesammelt wurden, der zum Bereitstellen neuer Server genutzt wird. Lesen Sie dazu Erstellen eines neuen Hardwareprofils.

Erstellen eines Hypervisor-Profils — Enthält die Hypervisor-Installationsinformationen, die für die ESX/ESXi-Bereitstellung erforderlich sind. Lesen Sie auch Erstellen eines neuen Hypervisor-Profils.

Erstellen einer Bereitstellungsvorlage — Enthält optional ein Hardwareprofil, ein Hypervisor-Profil oder beides. Sie können diese Profile bei Bedarf speichern und für alle verfügbaren Datacenter-Server erneut verwenden. Lesen Sie dazu auch Erstellen von Bereitstellungsvorlagen.

Nachdem eine Bereitstellungsvorlage erstellt wurde, verwenden Sie den Bereitstellungsassistenten, um die notwendigen Informationen zu sammeln, die zum Erstellen eines geplanten Auftrags erforderlich sind, um Serverhardware einzurichten und neue Hosts im vCenter bereitzustellen. Weitere Informationen zum Ausführen des Bereitstellungsassistenten finden Sie unter Ausführen des Bereitstellungsassistenten. Abschließend verwenden Sie die Job-Warteschlange, um den Auftragsstatus anzuzeigen und Änderungen an ausstehenden Bereitstellungsaufträgen vorzunehmen.



ANMERKUNG: Es sollten nicht mehr als zwei Bereitstellungsaufträge zur gleichzeitigen Ausführung geplant werden. Mehrere Aufgaben sollten die Planungsfunktion nutzen, um die Bereitstellungen nacheinander auszuführen.

Erforderliche Zeit für Bereitstellungs-Jobs

Die Einrichtung und Bereitstellung von Bare-Metal-Servern kann abhängig von bestimmten Faktoren zwischen 30 Minuten und mehreren Stunden dauern. Beim Starten eines Bereitstellungs-Jobs sollten Sie Ihre Bereitstellungszeit anhand der aufgeführten Richtwerte planen. Die erforderliche Zeit für eine vollständige Einrichtung und Bereitstellung hängt von Bereitstellungstyp, der Komplexität und der Anzahl an gleichzeitig ausgeführten Bereitstellungs-Jobs ab. Die folgenden Tabelle enthält Richtwerte für die ungefähre Dauer für eine Bereitstellungs-Jobs. Bereitstellungs-Jobs werden in Batches von bis zu fünf gleichzeitigen Servern ausgeführt, um die insgesamt erforderliche Zeit für die Bereitstellung zu verringern. Die genaue Anzahl an gleichzeitigen Jobs hängt von den verfügbaren Ressourcen ab.

Tabelle 2. Mögliche Zeitszenarios für Bereitstellungs-Jobs

Bereitstellungstyp	Ungefähre Zeit pro Bereitstellung
Nur Hypervisor	Zwischen 30 Minuten und 130 Minuten

Nur Hardware	Bis zu zwei Stunden, abhängig von der Komplexität und den zu konfigurierenden RAID-, BIOS- und Boot-Optionen
Hypervisor- und Hardware-Profile	1 bis 4 Stunden

Server-Status innerhalb der Bereitstellungssequenz

Wenn ein Auftrag zum Erstellen einer Bestandsliste ausgeführt wird, werden automatisch erfasste Bare-Metal-Systeme in unterschiedlichen Status klassifiziert, um feststellen zu können, ob der Server neu zum Datacenter hinzugefügt wurde oder ob eine ausstehende Bereitstellung geplant ist. Administratoren können anhand dieser Status feststellen, ob ein Server mit in einen Bereitstellungsauftrag aufgenommen werden sollte. Die möglichen Status sind:

Nicht konfiguriert	Der Server hat das OpenManage Integration for VMware vCenter kontaktiert und wartet auf die Konfiguration. Lesen Sie dazu auch Erforderliche Zeit für Bereitstellungsauftrag.
Konfiguriert	Der Server wurde mit allen Hardwareinformationen konfiguriert, die für eine erforderliche Hypervisor-Bereitstellung erforderlich sind.

Herunterladen von benutzerdefinierten Dell ISO-Images

Für die Bereitstellung werden benutzerdefinierte ESXi-Images benötigt, die *alle* Dell-Treiber enthalten. Dell ist nicht in der Lage, benutzerdefinierte ESX 4.1-Images zu erstellen. Damit Bereitstellungen funktionieren, müssen *alle* Treiber nativ in dem ISO-Image vorhanden sein, das von VMware produziert wird. Eine aktuelle Liste mit allen unterstützten ESXi-Versionen für diese Version finden Sie in den Versionshinweisen.



ANMERKUNG: DasOpenManage Integration for VMware vCenter ISO-Image enthält keine für die Bereitstellung erforderlichen benutzerdefinierten ESXi-ISO-Images. Sie müssen diese Images auf einen Speicherort herunterladen, auf den während der Bereitstellung zugegriffen werden kann, anderenfalls schlägt die Bereitstellung fehl.

1. Rufen Sie die Seite **support.dell.com** auf.
2. Suchen Sie die Seite **Treiber und Downloads** in Ihrer Sprache und führen Sie einen der folgenden Schritte aus:
   - Geben Sie zum Auswählen der Treiber unter Verwendung der Service-Tag-Nummer oder des Express-Service-Codes unter **Ja** die Service-Tag-Nummer oder den Express-Servicecode in das Textfeld ein und klicken Sie auf **Senden**.
   - Wählen Sie eine der folgenden Optionen unter **Nein** aus, um die Treiber unter Verwendung einer der anderen Optionen auszuwählen:
     - Service-Tag-Nummer automatisch ermitteln
     - Aus Liste My Products and Services (Meine Produkte und Services) auswählen
     - Aus allen Dell-Produkten auswählen

     Klicken Sie dann auf **Weiter** und befolgen Sie die Anweisungen für die gewählte Option.
3. Auf der Seite für den ausgewählten Server scrollen Sie bis **Ergebnisse präzisieren** und wählen unter **Betriebssystem** das gewünschte ESX- oder ESXi-System in der Dropdown-Liste aus.
4. Klicken Sie auf **Enterprise-Lösungen**.
5. Wählen Sie in der Liste **Enterprise-Lösungen** die Version des erforderlichen ISO aus und klicken Sie dann auf **Datei herunterladen**.

   ANMERKUNG: Eingebettete ISOs werden für Hypervisor-Installationen auf Dual Internal SD-Modulen verwendet. Installierbare ISOs dienen für Installationen auf Festplatten.
6. Wählen Sie in dem Dialogfeld **Für Download einer einzelnen Datei über den Browser** aus und klicken Sie anschließend auf **Jetzt herunterladen**.

7. Geben Sie in dem Dialogfeld den Speicherort für die ISO-Images für die Bereitstellung an.

Konfigurieren eines Hardwareprofils

Zum Konfigurieren der Serverhardwareeinstellungen müssen Sie zunächst ein Hardwareprofil erstellen. Ein Hardwareprofil ist eine Konfigurationsvorlage, die Sie an neu ermittelten Infrastrukturkomponenten anwenden können. Für ein Hardwareprofil sind die folgenden Informationen erforderlich:

Boot-Reihenfolge
Die Boot-Reihenfolge ist die Reihenfolge der Boot-Geräte und Festplatten, die Sie nur dann bearbeiten können, wenn der Boot-Modus auf BIOS gesetzt ist.

BIOS-Einstellungen
Die BIOS-Einstellungen umfassen: Speicher, Prozessor, SATA, integrierte Geräte, serielle Kommunikation, eingebettete Serververwaltung, Energieverwaltung, Systemsicherheit und verschiedene andere Einstellungen.

iDRAC Settings (iDRAC-Einstellungen)
Die iDRAC-Einstellungen umfassen: Netzwerk, Benutzerliste und Benutzerkonfiguration (IPMI/iDRAC-Rechte).



ANMERKUNG: Bei Systemen, die mit iDRAC Express ausgestattet sind, kann die iDRAC-Konfiguration nicht extrahiert werden. Aus diesem Grund darf der Server nicht als Referenzserver verwendet werden. Wird das System als Zielsystem verwendet, wird keine iDRAC-Konfiguration vom Referenzserver übernommen.

RAID-Konfiguration
Die RAID-Konfiguration zeigt die aktuelle RAID-Topologie auf dem Referenzserver zu dem Zeitpunkt an, an dem das Hardwareprofil extrahiert wurde.



ANMERKUNG: Im Hardware-Profil stehen zwei RAID-Konfigurationsoptionen zur Verfügung: 1. *RAID1 anwenden + ein dediziertes Hotspare erstellen, anwendbar*. Verwenden Sie diese Option, wenn Sie Standard-RAID-Konfigurationseinstellungen auf den Zielserver anwenden möchten. Die RAID-Konfigurationsaufgabe nimmt standardmäßig RAID1 auf den ersten zwei RAID-fähigen Laufwerken des integrierten Controllers an. Darüber hinaus wird ein dediziertes Ersatzgerät für das RAID1-Array angelegt, wenn ein Kandidatenlaufwerk die bestehenden Kriterien erfüllt. 2. *RAID-Konfiguration vom Referenzserver klonen, wie unten gezeigt*. Verwenden Sie diese Option, wenn Sie die Referenzservereinstellungten klonen möchten. Siehe Erstellen eines neuen Hardwareprofils.



ANMERKUNG: Das OpenManage Integration for VMware vCenter ermöglicht unter der Gruppe „Processor“ im BIOS bestimmte BIOS-Einstellungen für alle bereitgestellten Server, unabhängig von den Einstellungen auf dem Referenzserver. Bevor Sie einen Referenzserver zum Erstellen eines neuen Hardwareprofils verwenden, muss die „Collect System Inventory On Reboot“ (CSIOR)-Einstellung aktiviert und ein Neustart durchgeführt werden, um eine exakte Bestandsliste und Konfigurationseinstellungen zu erstellen.

Die Aufgaben zum Erstellen von Hardwareprofilen umfassen:

- Aktivieren von CSIOR auf einem Referenzserver
- Erstellen eines neuen Hardwareprofils
- Klonen eines neuen Hardwareprofils
- Allgemeines zum Verwalten von Hardwareprofilen

Erstellen eines neuen Hardwareprofils

So erstellen Sie ein neues Hardwareprofil:

1. Wählen Sie im Dell Management Center **Bereitstellung** → **Bereitstellungsvorlagen** → **Hardwareprofile** aus.
2. Klicken Sie auf **Neu erstellen**.
3. Führen Sie auf der Seite **Neues Hardwareprofil** Folgendes aus:
   - Geben Sie den Profilnamen in das Textfeld **Profilname** ein.
   - Geben Sie optional eine Beschreibung in das Textfeld **Beschreibung** ein.
4. Klicken Sie auf **Speichern**.
5. Klicken Sie zum Fortsetzen im linken Fensterbereich auf **Referenzserver**.
6. Klicken Sie im Fenster „Referenzserver" auf **Bearbeiten**.
7. Klicken Sie zum Suchen eines konformen Referenzservers, der von vCenter verwaltet wird und erfolgreich vom OpenManage Integration for VMware vCenter inventarisiert wurde, auf **Durchsuchen.**
8. Scrollen Sie im Dialogfeld **Server** durch die Liste, bis Sie den richtigen Referenzserver gefunden haben, und klicken Sie auf **Auswählen**.
9. Klicken Sie zum Anpassen der Referenzservereinstellungen als Standardeinstellungen zunächst auf **Benutzerdefinierte Einstellungen vom Referenzserver herstellen** und dann auf **Speichern**.
10. Ein Dialogfeld zeigt an, dass das Extrahieren der Einstellungen einige Minuten dauern wird. Klicken Sie auf **Weiter** um die Einstellungen zu verbreiten. Der Name des ausgewählten Servers, die iDRAC IP-Adresse sowie die Service-Tag-Nummer werden im Fenster **Referenzserver** angezeigt.
11. Wählen Sie im linken Fensterbereich **Startreihenfolge** aus. Aktivieren Sie das Kontrollkästchen **Startreihenfolge in Hardwareprofil einbeziehen**, um die Informationen zur Startreihenfolge in das Profil aufzunehmen.
12. Erweitern Sie **Startreihenfolge**, um die Optionen zur Startreihenfolge anzuzeigen, und klicken Sie auf **Bearbeiten**, um Aktualisierungen vorzunehmen:

    ANMERKUNG: Für Dell PowerEdge-Server der 13. Generation werden nur die Details des aktuellen Startmodus für die Hardwareprofile angezeigt.

    ANMERKUNG: Betriebssystembereitstellung von OpenManage Integration for VMware vCenter schlägt fehl, wenn der Boot-Modus auf dem Ziel-Computer auf UEFI gesetzt ist

    a. Wählen Sie in der Dropdown-Liste **Boot Mode** (Boot-Modus) entweder BIOS oder UEFI aus.
    b. Nehmen Sie Änderungen an der angezeigten Startreihenfolge in der Dropdown-Liste **Ansicht/Konfigurieren** unter **Startgerät-Reihenfolge** vor. Dazu wählen Sie das Gerät aus und klicken entweder auf **Nach oben** oder **Nach unten**.
    c. Wählen Sie in der Dropdown-Liste **Wiederholen der Startreihenfolge** die Option **Aktiviert** aus, so das der Server die Startreihenfolge automatisch erneut versucht, oder wählen Sie **Deaktiviert**, um die Reihenfolge nicht erneut auszuführen.
    d. Klicken Sie zum Speichern der Änderungen auf **Speichern** oder klicken Sie auf **Abbrechen**, um die Änderungen zu verwerfen.
13. Wenn der **BIOS-Startmodus** ausgewählt wurde, können Sie **Reihenfolge der Festplatten** erweitern, um die Auswahloptionen für Festplatten anzuzeigen. Klicken Sie dann auf **Bearbeiten**, um Änderungen vorzunehmen:
    - Um Änderungen an der angezeigten Reihenfolge der Festplatten vorzunehmen, wählen Sie das Gerät aus und klicken dann entweder auf **Nach oben** oder **Nach unten**.
    - Klicken Sie zum Speichern der Änderungen auf **Speichern** oder klicken Sie auf **Abbrechen**, um die Änderungen zu verwerfen.
14. Wählen Sie im linken Fensterbereich **BIOS-Einstellungen** aus. Aktivieren Sie das Kontrollkästchen **BIOS-Einstellungen in das Hardwareprofil einbeziehen**, um die BIOS-Einstellungen in das Profil aufzunehmen. Erweitern

Sie eine Kategorie, um die möglichen Einstellungen anzuzeigen, und klicken Sie auf **Bearbeiten**, um Aktualisierungen an einer der folgenden Optionen vorzunehmen:

- Speichereinstellungen
- Prozessoreinstellungen
- SATA-Einstellungen
- Integrierte Geräte
- Serielle Kommunikation
- Integrierte Serververwaltung
- Stromverwaltung
- Systemsicherheit
- Verschiedene Einstellungen

Nachdem alle Aktualisierungen an einer Kategorie vorgenommen wurden, klicken Sie auf **Übernehmen**, um die Änderungen zu speichern, oder auf **Abbrechen**, um die Änderungen zu verwerfen.

 **ANMERKUNG:** Ausführliche BIOS-Informationen, einschließlich möglicher Einstellungen und Erklärungen finden Sie im *Hardware-Bedienungshandbuch* für den ausgewählten Server.

15. Wählen Sie im linken Bereich **iDRAC-Einstellungen** aus, und klicken Sie auf **Netzwerk**.
16. Aktivieren Sie das Kontrollkästchen **Netzwerk-Einstellungen in das Hardwareprofil einbeziehen**, um die Netzwerkeinstellungen in das Profil aufzunehmen. Erweitern Sie eine Kategorie, um die möglichen Einstellungen anzuzeigen, und klicken Sie auf **Bearbeiten**, um Aktualisierungen an einer der folgenden Optionen vorzunehmen:

   - Netzwerk
   - Netzwerkeinstellungen
   - Virtueller Datenträger

   Nachdem alle Aktualisierungen an einer Kategorie vorgenommen wurden, klicken Sie auf **Übernehmen**, um die Änderungen zu speichern, oder auf **Abbrechen**, um die Änderungen zu verwerfen.

    **ANMERKUNG:** Ausführliche iDRAC-Informationen, einschließlich möglicher Einstellungen und Erklärungen, finden Sie im *iDRAC-Benutzerhandbuch* für den ausgewählten Server.

17. Wählen Sie im linken Fensterbereich **iDRAC-Einstellungen** → **Benutzerliste** aus. Aktivieren Sie das Kontrollkästchen **Benutzerliste in das Hardwareprofil einbeziehen**, um die Informationen zur Startreihenfolge in das Profil aufzunehmen. Unter „Liste der lokalen iDRAC-Benutzer" führen Sie einen der folgenden Schritte aus:
   a. **Benutzer hinzufügen**: Geben Sie manuell einen iDRAC-Benutzer und die erforderlichen Informationen ein. Klicken Sie anschließend auf **Speichern**, um Ihre Änderungen zu speichern, oder auf **Abbrechen**, um die Änderungen zu verwerfen.
   b. **Benutzer löschen**: Löscht den ausgewählten Benutzer. Aktivieren Sie das Kontrollkästchen für den Benutzer und klicken Sie auf **Löschen**, um den ausgewählten Benutzer zu löschen, oder auf **Abbrechen**, um die Änderungen zu verwerfen.
   c. **Benutzer bearbeiten**: Bearbeiten Sie manuell die Informationen zu einem iDRAC-Benutzer. Klicken Sie anschließend auf **Speichern**, um die Änderungen zu speichern, oder auf **Abbrechen**, um die Änderungen zu verwerfen.

    **ANMERKUNG:** Ausführliche iDRAC-Informationen, einschließlich möglicher Einstellungen und Erklärungen, finden Sie im *iDRAC-Benutzerhandbuch* für den ausgewählten Server.

18. Wählen Sie im linken Fenster **RAID-Konfiguration** aus. Aktivieren Sie das Kontrollkästchen **RAID-Konfiguration in das Hardwareprofil einbeziehen**, um die RAID-Konfigurationsinformationen in das Profil aufzunehmen. Wählen Sie dann eine der folgenden Optionen aus.

   - RAID1 anwenden + ein dediziertes Hotspare erstellen, anwendbar.

     Verwenden Sie diese Option, wenn Sie Standard-RAID-Konfigurationseinstellungen auf den Zielserver anwenden möchten. Die RAID-Konfigurationsaufgabe nimmt standardmäßig RAID1 auf den ersten zwei RAID-

fähigen Laufwerken des integrierten Controllers an. Darüber hinaus wird ein dediziertes Ersatzgerät für das RAID1-Array angelegt, wenn ein Kandidatenlaufwerk die bestehenden Kriterien erfüllt.

- RAID-Konfiguration vom Referenzserver klonen.

  Verwenden Sie diese Option, wenn Sie die Referenzservereinstellungten klonen möchten.

Das Profil wird automatisch gespeichert und zeigt das Fenster **Hardwareprofile** unter **Verfügbare Profile** an.

Aktivieren von CSIOR auf einem Referenzserver

Bevor Sie ein Hardwareprofil mit einem Referenzserver erstellen, aktivieren Sie die Einstellung „Collect System Inventory On Reboot“ (CSIOR) und booten Sie den Server neu, um die korrekten Informationen zur Bestandsliste und Konfiguration bereitzustellen. Es gibt zwei Methoden zum Aktivieren von CSIOR:

Lokal — Hier wird ein individueller Host mit der Benutzeroberfläche „Dell Lifecycle Controller United Server Configurator“ (USC) verwendet.

Remote — Hier wird ein WS-Man-Skript verwendet. Weitere Informationen zu dieser Funktion finden Sie im *Dell Tech Center* und unter *DCIM Lifecycle Controller Management-Profil*.

So aktivieren Sie CSIOR lokal auf einem Referenzserver:

1. Schalten Sie das System ein und drücken Sie während des POST die Taste **<F10>**, um USC zu starten.
2. Wählen Sie **Hardwarekonfiguration** → **Teileaustauschkonfiguration**.
3. Aktivieren Sie die Einstellung **Bestandsliste des Systems beim Neustart erstellen** und beenden Sie USC.

Klonen eines Hardwareprofils

So klonen Sie ein neues Hardwareprofil:

1. Wählen Sie im Dell Management Center **Bereitstellung** → **Bereitstellungsvorlagen** → **Hardwareprofile** aus.
2. Klicken Sie auf **Neu erstellen**.
3. Führen Sie auf der Seite **Neues Hardwareprofil** Folgendes aus:
   - Geben Sie den Profilnamen in das Textfeld **Profilname** ein
   - Geben Sie optional eine Beschreibung in das Textfeld **Beschreibung** ein.
4. Klicken Sie auf **Speichern**.
5. Klicken Sie im linken Fensterbereich auf **Referenzserver**.
6. Klicken Sie im Fenster **Referenzserver** auf **Bearbeiten**.
7. Klicken Sie auf das Optionsfeld **Einstellungen für geklonten Referenzserver**, um alle Hardwareeinstellungen des Referenzservers zu extrahieren.
8. Klicken Sie auf **Speichern**.
9. Ein Dialogfeld zeigt an, dass das Extrahieren der Einstellungen einige Minuten dauern wird. Klicken Sie auf **Weiter**. Die Einstellungen werden verbreitet und der Name des ausgewählten Servers, die iDRAC IP-Adresse sowie die Service-Tag-Nummer werden im Fenster „Referenzserver“ angezeigt.

   Das Profil wird gespeichert und zeigt das Fenster **Hardwareprofile** unter **Verfügbare Profile** an.

Allgemeines zum Verwalten von Hardwareprofilen

Hardwareprofile definieren die Hardwarekonfiguration eines Servers mithilfe eines Referenzservers. Im Dell Management Center gibt es verschiedene Verwaltungsaktionen, die Sie an vorhandenen Hardwareprofilen durchführen können. Dazu gehören:

- Anzeigen bzw. Bearbeiten eines Hardwareprofils

- [Duplizieren von Hardwareprofilen]
- [Umbenennen eines Hardwareprofils]
- [Löschen eines Hardwareprofils]
- [Aktualisieren von Hardwareprofilen]

Anzeigen bzw. Bearbeiten eines Hardwareprofils

So zeigen Sie ein Hardwareprofil an bzw. nehmen Änderungen daran vor:

1. Wählen Sie im Dell Management Center **Bereitstellung** → **Bereitstellungsvorlagen** → **Hardwareprofile** aus.
2. Wählen Sie einen Profil aus und klicken Sie auf **Anzeigen/Bearbeiten**.
3. Klicken Sie im Fenster **Hardwareprofils** auf **Bearbeiten**, um Änderungen vorzunehmen.
4. Klicken Sie zum Speichern der Änderungen auf **Speichern**, oder auf **Abbrechen**, um die Änderungen zu verwerfen.

Duplizieren eines Hardwareprofils

So duplizieren Sie ein Hardwareprofils:

1. Wählen Sie im Dell Management Center **Bereitstellung** → **Bereitstellungsvorlagen** → **Hardwareprofile** aus.
2. Wählen Sie auf der Seite **Hardwareprofil** ein Profil aus und klicken Sie auf **Duplizieren**.
3. Geben Sie einen einmaligen Hardwareprofilnamen in das Dialogfeld **Duplizieren** ein.
4. Klicken Sie auf **Übernehmen**, um eine Kopie des Profils mit dem neuen Namen zu erstellen, oder klicken Sie auf **Abbrechen**, um den Vorgang abzubrechen.

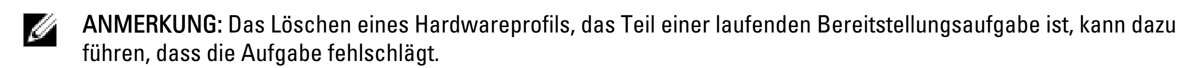
Umbenennen eines Hardwareprofils

So benennen Sie ein Hardwareprofil um:

1. Wählen Sie im Dell Management Center**Bereitstellung** → **Bereitstellungsvorlagen** → **Hardwareprofile** aus.
2. Wählen Sie auf der Seite **Hardwareprofil** ein Profil aus und klicken Sie auf **Umbenennen**.
3. Geben Sie einen einmaligen Hardwareprofilnamen in das Dialogfeld **Umbenennen** ein.
4. Klicken Sie auf **Übernehmen**, um den neuen Namen zu verwenden, oder klicken Sie auf **Abbrechen**, um die Änderungen zu verwerfen.

Löschen eines Hardwareprofils

So löschen Sie ein Hardwareprofil:



ANMERKUNG: Das Löschen eines Hardwareprofils, das Teil einer laufenden Bereitstellungsaufgabe ist, kann dazu führen, dass die Aufgabe fehlschlägt.

1. Wählen Sie im Dell Management Center **Bereitstellung** → **Bereitstellungsvorlagen** → **Hardwareprofile** aus.
2. Wählen Sie einen Profil aus und klicken Sie auf **Löschen**.
3. Klicken Sie in der folgenden Bestätigungsmeldung entweder auf **Löschen** oder auf **Abbrechen**.

Aktualisieren eines Hardwareprofils

So aktualisieren Sie ein Hardwareprofil:

1. Wählen Sie im Dell Management Center**Bereitstellung** → **Bereitstellungsvorlagen** → **Hardwareprofile** aus.
2. Klicken Sie auf **Aktualisieren.**

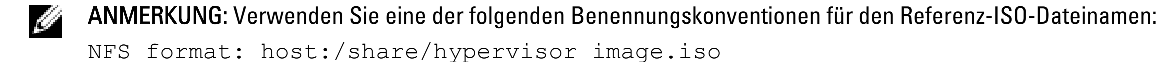
Die aktualisierten Hardwareprofil-Informationen werden angezeigt.

Neues Hypervisor-Profil erstellen

Zum Bereitstellen und Konfigurieren von ESX/ESXi auf einem Server muss ein Hypervisor-Profile erstellt werden. Ein Hypervisor-Profil benötigt die folgenden Informationen:

- Den Speicherort des skriptfähigen Referenz-ISO-Softwaremediums auf einer NFS- oder CIFS-Freigabe
- Die vCenter-Instanz, die die bereitgestellten Hosts verwaltet, sowie ein optionales Hostprofil
- Das Ziel-Cluster oder -Datacenter, in dem das Plugin Server in vCenter bereitstellt

ANMERKUNG: Verwenden Sie eine der folgenden Benennungskonventionen für den Referenz-ISO-Dateinamen:



`NFS format: host:/share/hypervisor_image.iso`



`CIFS format: \\host\share\hypervisor.iso`

ANMERKUNG: Eine erfolgreiche Bereitstellung erfordert ein ESX ISO, das über die richtigen Treiber verfügt. Die Bereitstellung auf neueren Dell-Systemen kann die Verwendung von benutzerdefinierten Dell ISO-Images verlangen, die alle erforderlichen Dell-Treiber enthalten. Eventuell kann ESX 4.1 auf neueren Dell-Systemen nicht eingesetzt werden und möglicherweise steht kein benutzerdefiniertes ISO von Dell zur Verfügung.

So erstellen Sie ein neues Hypervisor-Profil:

1. Wählen Sie im **Dell Management Center Bereitstellung** → **Bereitstellungsvorlagen** → **Hardwareprofil** aus.
2. Klicken Sie auf der Seite **Hypervisor-Profile** auf **Neu erstellen**.
3. Führen Sie auf der Seite **Neues Hypervisor-Profil** Folgendes aus:
   - Geben Sie den Profilnamen in das Textfeld **Profilname** ein.
   - Geben Sie optional eine Beschreibung in das Textfeld **Beschreibung** ein.
4. Klicken Sie im linken Bereich auf **Referenz-ISO**. Klicken Sie dann auf **Bearbeiten** und geben Sie im Dialogfeld **Hypervisor-Installationsquelle** die folgenden Informationen ein:
   - Geben Sie den Pfad zum Speicherort Ihrer Hypervisor-Freigabe in das Textfeld **Installationsquelle-ISO** ein. Eine Kopie dieses Hypervisor-Images wird modifiziert, um eine skriptgeführte Installation zuzulassen. Der Speicherort für das Referenz-ISO muss die folgende Syntax aufweisen:

     NFS-Format: host:/freigabe/hypervisor_image.iso

     CIFS-Format: \\host\freigabe\hypervisor.iso
   - Wählen Sie in der Dropdown-Liste **Version auswählen** eine ESX- oder ESXi-Version.

   Alle Server, die mit diesem Hypervisor-Profil bereitgestellt werden, verfügen über dieses Image. Wenn die Server eine Version vor 12G aufweisen, wird die letzte empfohlene Version von OpenManage Server Administrator installiert.
5. Wenn Sie eine CIFS-Freigabe verwenden, geben Sie Werte in die Felder **Benutzername, Kennwort Kennwort bestätigen** ein. Die Kennwörter müssen übereinstimmen.
6. Klicken Sie auf **Speichern**, um die Einstellungen zum Profil hinzuzufügen.
7. Klicken Sie im linken Fensterbereich auf **vCenter-Einstellungen** und ggf. auf Bearbeiten:
   - **vCenter-Instanz**: Zeigt die Server-Instanz an, die einen Host nach der Bereitstellung verwaltet.
   - **vCenter-Version**: Zeigt die aktuelle Version an.
   - **vCenter-Ziel-Container**: Datacenter oder Cluster, das als Host für die neuen physischen Server fungiert; klicken Sie auf **Durchsuchen**, um nach den vCenter-Zielen zu suchen.
   - **vCenter-Hostprofil**: Wählen Sie ein Profil aus, das eine Hostkonfiguration enthält und das Verwalten der Hostkonfiguration unterstützt.

8. Klicken Sie auf **Speichern**, um die Informationen zum Profil hinzuzufügen.

Weitere Informationen zum Verwalten von Hypervisor-Profilen finden Sie unter Verwalten von Hypervisor-Profilen.

Verwalten von Hypervisor-Profilen

Es gibt verschiedene Verwaltungsmaßnahmen, die Sie an bestehenden Hypervisor-Profilen vornehmen können. Dazu gehören:

- VLAN-Support verstehen
- Anzeigen bzw. Bearbeiten eines Hypervisor-Profils
- Duplizieren eines Hypervisor-Profils
- Umbenennen eines Hypervisor-Profils
- Löschen eines Hypervisor-Profils
- Aktualisieren eines Hypervisor-Profils

VLAN-Support

Das OpenManage Integration for VMware vCenter unterstützt die Hypervisor-Bereitstellung zu einem umleitbaren VLAN. Konfigurieren Sie den VLAN-Support im Bereitstellungsassistenten. In diesem Teil des Bereitstellungsassistenten gibt es eine Option, in der Sie die Verwendung von VLANs und eine VLAN-ID angeben können. Wenn eine VLAN-ID bereitgestellt wird, wird sie während der Bereitstellung auf die Verwaltungsschnittstelle des Hypervisors angewandt und markiert den ganzen Verkehr mit der VLAN-ID.

Achten Sie darauf, dass das während der Bereitstellung bereitgestellte VLAN mit dem virtuellen Gerät sowie mit dem vCenter-Server kommuniziert. Die Bereitstellung eines Hypervisor für ein VLAN, das nicht mit einem oder beiden dieser Ziele kommunizieren kann, führt dazu, dass die Bereitstellung fehlschlägt.

Falls Sie mehrere Bare-Metal-Server in einem einzelnen Bereitstellungs-Job ausgewählt haben und dieselbe VLAN-ID auf alle Server anwenden möchten, dann verwenden Sie im Serveridentifizierungsteil des Bereitstellungsassistenten die Schaltfläche *Einstellungen auf alle ausgewählten Server anwenden*. Diese Option ermöglicht Ihnen die Anwendung derselben VLAN-ID zusammen mit den anderen Netzwerkeinstellungen auf alle Server im betreffenden Bereitstellungs-Job.



ANMERKUNG: Das OpenManage Integration for VMware vCenter unterstützt eine multi-homed Konfiguration nicht. Das Hinzufügen einer zweiten Netzwerkschnittstelle zum Gerät für die Kommunikation mit einem zweiten Netzwerk verursacht Probleme für den Arbeitsfluss, und zwar mit der Hypervisor-Bereitstellung, der Server-Übereinstimmung und Firmware-Aktualisierungen.

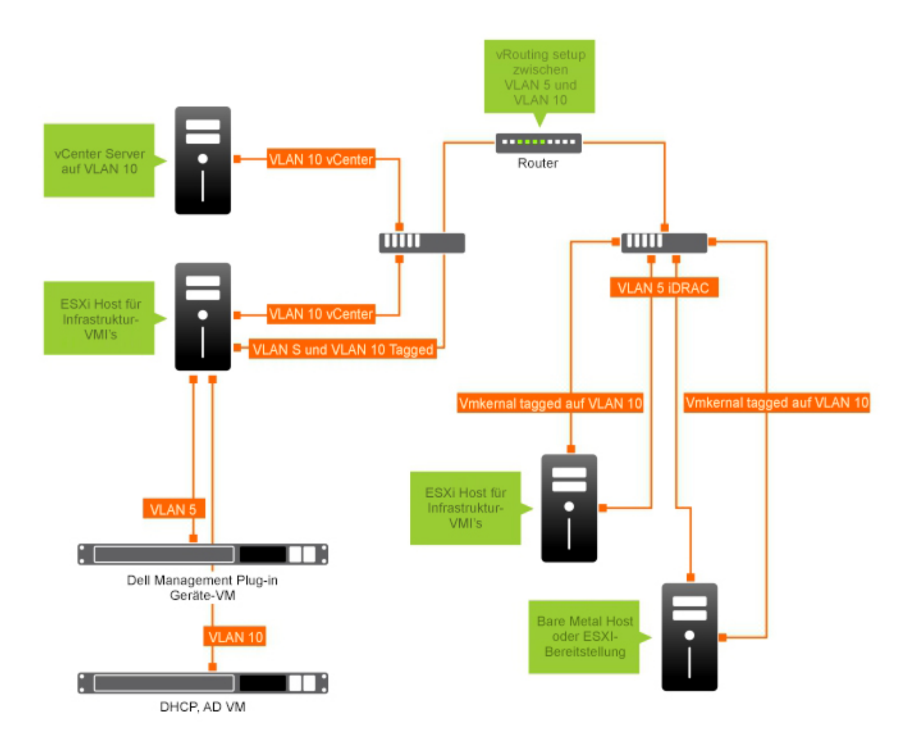


Abbildung 4. Beispiel eines VLAN-Netzwerks.

In diesem Beispielnetzwerk befindet sich das OpenManage Integration for VMware vCenter auf einem VLAN 5, während das vCenter und der VMkernal der ESXi-Hosts auf VLAN 10 bereitgestellt werden. Da das OpenManage Integration for VMware vCenter das Multi-VLAN-Homing nicht unterstützt, muss VLAN 5 für alle Systeme auf VLAN 10 umgeleitet werden, damit sie korrekt miteinander kommunizieren können. Falls das Routing zwischen diesen VLANs nicht aktiviert ist, schlägt die Bereitstellung fehl.

Anzeigen bzw. Bearbeiten eines Hypervisor-Profils

So zeigen Sie ein Hypervisor-Profil an bzw. nehmen Änderungen daran vor:

1. Wählen Sie im Dell Management Center **Bereitstellung** → **Bereitstellungsvorlage** → **Hypervisor-Profile** aus.
2. Wählen Sie einen Profil aus und klicken Sie auf **Anzeigen/Bearbeiten**.
3. Wählen Sie im Fenster **Hypervisor-Profile: Profilname** den anzuzeigenden bzw. zu ändernden Profilabschnitt aus, und nehmen Sie die notwendigen Änderungen vor.
4. Klicken Sie zum Speichern der Änderungen auf **Speichern**, oder auf **Abbrechen**, um die Änderungen zu verwerfen.

Duplizieren eines Hypervisor-Profils

So duplizieren Sie ein Hypervisor-Profil:

1. Wählen Sie im Dell Management Center **Bereitstellung** → **Bereitstellungsvorlage** → **Hypervisor-Profile** aus.
2. Wählen Sie auf der Seite **Hypervisor-Profile** ein Profil aus und klicken Sie auf **Duplizieren** .
3. Geben Sie einen einmaligen Hypervisor-Profilnamen in das Dialogfeld **Duplizieren** ein.
4. Klicken Sie auf **Übernehmen**, um eine Kopie des Profils mit dem neuen Namen zu erstellen, oder klicken Sie auf **Abbrechen**, um den Vorgang abzubrechen.

Umbenennen eines Hypervisor-Profils

So benennen Sie ein Hypervisor-Profil um:

1. Wählen Sie im Dell Management Center**Bereitstellung** → **Bereitstellungsvorlagen** → **Hypervisor-Profile** aus.
2. Wählen Sie auf der Seite **Hypervisor-Profile** ein Profil aus und klicken Sie auf **Umbenennen**.
3. Geben Sie einen einmaligen Hypervisor-Profilnamen in das Dialogfeld **Umbenennen** ein.
4. Klicken Sie auf **Übernehmen**, um den neuen Namen zu verwenden, oder klicken Sie auf **Abbrechen**, um die Änderungen zu verwerfen.

Löschen eines Hypervisor-Profils

So löschen Sie ein Hypervisor-Profil:



ANMERKUNG: Das Löschen eines Hypervisor-Profils, das Teil einer laufenden Bereitstellungsaufgabe ist, kann dazu führen, dass die Aufgabe fehlschlägt.

1. Wählen Sie im Dell Management Center **Bereitstellung** → **Bereitstellungsvorlagen** → **Hypervisor-Profile** aus.
2. Wählen Sie einen Profil aus und klicken Sie auf **Löschen**.
3. Klicken Sie in der folgenden Bestätigungsmeldung entweder auf **Löschen** , um das Profil zu löschen, oder auf **Abbrechen**, um den Vorgang abzubrechen.

Aktualisieren eines Hypervisor-Profils

So aktualisieren Sie ein Hypervisor-Profil:

1. Wählen Sie im Dell Management Center **Bereitstellung** → **Bereitstellungsvorlagen** → **Hypervisor-Profile** aus.
2. Klicken Sie auf **Aktualisieren.**

   Die aktualisierten Hypervisor-Profil-Informationen werden angezeigt.

Erstellen einen neuer Bereitstellungsvorlage

Eine Bereitstellungsvorlage enthält entweder ein Hardwareprofil, ein Hypervisor-Profil oder beides. Der Bereitstellungsassistent verwendet diese Vorlage, um Serverhardware einzurichten und Hosts innerhalb von vCenter bereitzustellen.

So erstellen Sie eine neue Bereitstellungsvorlage:

1. Wählen Sie im Dell Management Center**Bereitstellung** → **Bereitstellungsvorlagen**aus.
2. Klicken Sie unter **Verfügbare Profile** auf **Neu erstellen**.
3. Geben Sie einen Namen für die Vorlage in das Fenster **Neu erstellen** ein und klicken Sie auf **Speichern**.
4. Klicken Sie zum Fertig stellen der Vorlage auf **Bearbeiten**.
5. Wählen Sie im rechten Fensterbereich ein Profil in der Dropdown-Liste **Profil** aus und führen Sie dann einen der folgenden Schritte aus:

   - Klicken Sie auf **Anzeigen**, um die Hardware-/Hypervisor-Profileinstellungen für das ausgewählte Profil anzuzeigen.
   - Klicken Sie auf **Neu erstellen**, um ein neues Hardware-/Hypervisor-Profil zu erstellen.
6. Geben Sie optional eine **Beschreibung** für die Bereitstellungsvorlage ein.
7. Klicken Sie zum Übernehmen der Profilauswahl und zum Speichern der Änderungen auf **Speichern**, oder klicken Sie auf **Abbrechen**, um die Änderungen zu verwerfen.

Verwalten von Bereitstellungsvorlagen

Es gibt verschiedene Verwaltungsmaßnahmen, die Sie im Dell Management Center an bestehenden Bereitstellungsvorlagen vornehmen können. Dazu gehören:

- Erstellen von Bereitstellungsvorlagen
- Duplizieren von Bereitstellungsvorlagen
- Umbenennen von Bereitstellungsvorlagen
- Löschen von Bereitstellungsvorlagen

Duplizieren von Bereitstellungsvorlagen

So duplizieren Sie eine Bereitstellungsvorlage:

1. Wählen Sie im Dell Management Center**Bereitstellung** → **Bereitstellungsvorlagen**aus.
2. Wählen Sie auf der Seite „Bereitstellungsvorlagen" eine Vorlage aus und klicken Sie auf **Duplizieren**.
3. Geben Sie den neuen Namen der Vorlage ein und klicken Sie auf **Anwernden**. Der Name der Vorlage darf nicht mehrfach vergeben werden.

Löschen von Bereitstellungsvorlagen

So löschen Sie eine Bereitstellungsvorlage:

1. Wählen Sie im Dell Management Center**Bereitstellung** → **Bereitstellungsvorlagen** aus.
2. Wählen Sie auf der Seite **Bereitstellungsvorlagen** eine Vorlage aus und klicken Sie auf **Löschen**.
3. Klicken Sie in der angezeigten Meldung auf **Löschen**, um die Vorlage zu löschen, oder klicken Sie auf **Abbrechen**, um den Vorgang abzubrechen.

Umbenennen einer Bereitstellungsvorlage

So benennen Sie eine Bereitstellungsvorlage um:

1. Wählen Sie im Dell Management Center **Bereitstellung** → **Bereitstellungsvorlagen** aus.
2. Wählen Sie auf der Seite **Bereitstellungsvorlagen** eine Vorlage aus und klicken Sie auf **Umbenennen**.
3. Geben Sie den neuen Namen der Vorlage ein und klicken Sie auf **Anwenden**. Der Name der Vorlage darf nicht mehrfach vergeben werden.
4. Wählen Sie zum Anzeigen aller Bereitstellungsvorlagen im **Dell Management Center Bereitstellung** → **Bereitstellungsvorlagen** aus und klicken Sie auf **Aktualisieren**.

Ausführen des Bereitstellungsassistenten

Der Bereitstellungsassistent führt Sie durch die Schritte zur Bereitstellung eines Bare-Metal-Servers:

- Wählen Sie noch nicht bereitgestellte Server aus.

  Wenn Sie einen Hypervisor bereitstellen, können Sie die Bereitstellung auf einem internen Dual SD-Modul mit einer minimalen Speicherkapazität von 1 GB durchführen. Bevor Sie einen Hypervisor mit dem OpenManage Integration for VMware vCenter bereitstellen können, muss das interne Dual SD-Modul im BIOS aktiviert werden.
- Verwenden einer Bereitstellungsvorlage (Kombination aus Hardware- und Hypervisor-Profilen).
- Richten Sie die globalen Einstellungen ein. Auf dieser Seite können Sie wählen, ob ein Hypervisor auf einer Festplatte oder einem internen Dual SD-Modul bereitgestellt werden soll.
- Zuweisen der Identifikation zu den bereitgestellten Servern.
- Zuordnen eines gewünschten Verbindungsprofils zu jedem Server.
- Planen der auszuführenden Serverbereitstellungsjobs.

- Anzeigen der Job-Warteschlange, mit der Sie Bereitstellungs-Jobs verwalten können.



ANMERKUNG: Wenn Sie nur ein Hardwareprofil bereitstellen, werden die Seiten „Neue globale Einstellungen", „Server-Identifikation" und „Verbindungsprofil" übersprungen, und Sie gelangen direkt zur Seite „Job planen".



ANMERKUNG: Mit einer Demo-/Test-Lizenz können Sie den Bereitstellungsassistenten für die Dauer Ihrer Lizenz verwenden.

Verwandte Aufgaben:

- Bereitstellungsassistent Schritt 1: Server auswählen
- Bereitstellungsassistent Schritt 2: Bereitstellungsvorlagen
- Bereitstellungsassistent Schritt 3: Globale Einstellungen
- Bereitstellungsassistent Schritt 4: Server-Identifikation
- Bereitstellungsassistent Schritt 5: Verbindungsprofil
- Bereitstellungsassistent Schritt 6: Jobs planen

Bereitstellungsassistent Schritt 1: Server auswählen

Diese Seite dient zur Server-Bereitstellung. Wenn Sie Hypervisor auf einem internen Dual SD-Modul diese Seite an, ob die Option verfügbar oder nicht verfügbar ist. Weitere Informationen zu internen Dual SD-Modulen finden Sie unter Ausführen des Bereitstellungsassistenten. Wenn die Server, die Sie bereitstellen möchten, die nicht in der Liste in Schritt 2 angezeigt werden, können Sie die Server manuell hinzufügen. Lesen Sie dazu Manuelles Hinzufügen eines Servers.
So wählen Sie Server aus:

1. Wählen Sie im **Dell Management Center Bereitstellung → Bereitstellungsvorlagenassistent**aus.
2. Weisen Sie im Fenster **Server auswählen** nicht bereitgestellte Server für diesen Auftrag aus. Aktivieren Sie dazu die Kontrollkästchen, um die **Server** auszuwählen.
3. Klicken Sie auf **Weiter.**

Klicken Sie auf Bereitstellungsassistent Schritt 2, um diese Aufgabe mit Schritt 2 fortzusetzen.

Bereitstellungsassistent Schritt 2: Bereitstellungsvorlagen

Bereitstellungen für ein Hardwareprofil weichen von Hypervisor-Bereitstellungen ab. Wenn Sie für ein Hardwareprofil bereitstellen, klicken Sie auf Bereitstellungsassistent Schritt 6.



ANMERKUNG: Eine erfolgreiche Bereitstellung erfordert ein ESX ISO, das über die richtigen Treiber verfügt. Die Bereitstellung auf neueren Dell-Systemen kann die Verwendung von benutzerdefinierten Dell ISO-Images verlangen, die alle erforderlichen Dell-Treiber enthalten. Eventuell kann ESX 4.1 auf neueren Dell-Systemen nicht eingesetzt werden und möglicherweise steht kein benutzerdefiniertes ISO von Dell zur Verfügung.

So wählen Sie eine Bereitstellungsvorlage aus:

1. Bereitstellungsvorlagen wählen/erstellen eine Bereitstellungsvorlage nach einer der folgenden Methoden:
   - Wählen Sie unter **Verfügbare Vorlagen** eine vorhandene Bereitstellungsvorlage aus. Die Informationen der ausgewählten Vorlage füllen die Felder im rechten Fensterbereich aus.
   - Wählen Sie eine vorhandene Bereitstellungsvorlage und klicken Sie auf **Bearbeiten**, um eines oder beide zugeordneten Profile zu bearbeiten.
   - Klicken Sie auf **Neu erstellen**, um eine neue Vorlage zu definieren.
2. Wählen Sie eine der folgenden Optionen:

- Wenn Sie für ein Hardwareprofil bereitstellen, klicken Sie auf **Weiter**. Sie gelangen zum Bereitstellungsassistent Schritt 6.
- Wenn Sie für ein Hypervisor-Profil bereitstellen, klicken Sie auf **Weiter**. Sie gelangen zum Bereitstellungsassistent Schritt 3.

Bereitstellungsassistent Schritt 3: Globale Einstellungen

Sie können einen Hypervisor entweder auf einem Festplattenlaufwerk oder einem internen Dual SD-Modul bereitstellen. Wenn ein internes Dual SD-Modul auf mindestens einem der ausgewählten Server verfügbar ist, wird die Option **interne Dual-SD-Modul** standardmäßig aktiviert. Wenn dies nicht der Fall ist, sind die Optionen **Festplatte** und **Internes Dual SD-Modul** nicht ausgewählt.

Um den Hypervisor bereitzustellen, führen Sie die folgenden Schritte aus:

1. Wählen Sie auf der Seite „Globale Einstellungen“ eine der folgenden Optionen aus:
   - **Festplatte** - Stellt den Hypervisor auf der Festplatte bereit.
   - **Internes Dual SD-Modul** – Stellt den Hypervisor auf dem internen Dual SD-Modul bereit.
2. Wenn einer der ausgewählten Server kein internes Dual SD-Modul unterstützt oder während der Bereitstellung kein internes Dual SD-Modul vorhanden ist, führen Sie eine der folgenden Aktionen aus:
   - Markieren Sie das Kontrollkästchen **Hypervisor auf der ersten Festplatte für die Server bereitstellen, die über kein internes Dual SD-Modul verfügen**, wenn Sie möchten, dass der Hypervisor auf der ersten Festplatte der Server bereitgestellt wird.

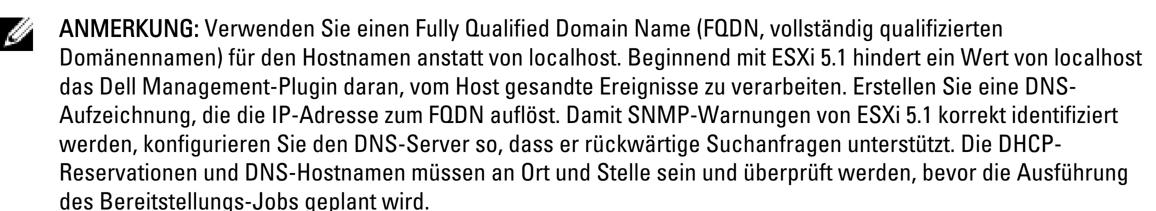
     VORSICHT: Wenn Sie diese Option auswählen und den Hypervisor auf der ersten Festplatte der Server bereitstellen, werden alle Daten auf den Festplattenlaufwerken gelöscht.
   - Deaktivieren Sie das Kontrollkästchen **Hypervisor auf der ersten Festplatte für die Server bereitstellen, die über kein internes Dual SD-Modul verfügen**, um die Bereitstellung auf diesen Servern zu überspringen und mit der Hypervisor-Bereitstellung auf dem nächsten Server fortzufahren.
3. Klicken Sie auf **Weiter**.

   Klicken Sie auf Bereitstellungsassistent Schritt 4: Server-Identifikation, um die Aufgabe mit Schritt 4 fortzusetzen.

Bereitstellungsassistent Schritt 4: Server-Identifikation

Die Server-Identifikation kann auf zwei Arten durchgeführt werden:

- Durch Eingabe der Netzwerkinformationen (IP Adresse, Subnetzmaske und Gateway); ein vollständig qualifizierter Domänenname für den Hostnamen ist obligatorisch. Die Verwendung von *localhost* für das FQDN wird nicht unterstützt. Das FQDN wird verwendet, wenn der Host dem vCenter hinzugefügt wird.
- Durch Verwenden des Dynamic Host Configuration Protocol (DHCP) zum Konfigurieren der IP-Adressen, Subnetzmaske, Gateway-IP, Hostname und bevorzugter/alternativer DNS-Server. Die von DHCP zugewiesene IP-Adresse wird verwendet, wenn der Host dem vCenter hinzugefügt wird. Bei der Verwendung von DHCP wird empfohlen, dass eine IP-Reservation für ausgewählte NIC MAC-Adressen verwendet werden.



ANMERKUNG: Verwenden Sie einen Fully Qualified Domain Name (FQDN, vollständig qualifizierten Domänennamen) für den Hostnamen anstatt von localhost. Beginnend mit ESXi 5.1 hindert ein Wert von localhost das Dell Management-Plugin daran, vom Host gesandte Ereignisse zu verarbeiten. Erstellen Sie eine DNS-Aufzeichnung, die die IP-Adresse zum FQDN auflöst. Damit SNMP-Warnungen von ESXi 5.1 korrekt identifiziert werden, konfigurieren Sie den DNS-Server so, dass er rückwärtige Suchanfragen unterstützt. Die DHCP-Reservationen und DNS-Hostnamen müssen an Ort und Stelle sein und überprüft werden, bevor die Ausführung des Bereitstellungs-Jobs geplant wird.

Dieser Bildschirm stellt die Option zur Angabe einer VLAN-ID bereit. Wenn eine VLAN-ID bereitgestellt wird, wird sie während der Bereitstellung auf die Verwaltungsschnittstelle des Hypervisors angewandt und markiert allen Datenverkehr mit der VLAN-ID.

So identifizieren Sie Ihren Server:

1. Die Server-Identifikation weist bereitgestellten Servern neue Namen und eine Netzwerkidentifikation zu. Klicken Sie auf **Nicht konforme Server**, um eine Liste der Server anzuzeigen, die die Mindestanforderungen an die Firmware oder das BIOS nicht erfüllen oder andere Probleme aufweisen.
2. Weitere Informationen erhalten Sie durch Klicken auf **Details**.
3. Nachdem die Systeme aktualisiert wurden, klicken Sie auf **Konformität prüfen**, um eine erneute Prüfung durchzuführen und Korrekturen zu verifizieren. Klicken Sie zum Aktualisieren der Liste auf **Aktualisieren** und auf **Alle Tests abbrechen**, um die Tests abzubrechen.
4. Klicken Sie auf ^, um die individuellen Serverinformationen zu erweitern und anzuzeigen.
5. Geben Sie unter **Hostname und NIC** einen **vollständig qualifizierten Hostnamen** für den Server ein.
6. Wählen Sie in der Dropdown-Liste **NIC Management Tasks** die Netzwerkschnittstellenkarte aus, die zur Verwaltung des Servers verwendet wird.
7. Geben Sie die **IP-Adressen**, **Subnetzmaske** und weitere Netzwerkinformationen ein, oder aktivieren Sie das Kontrollkästchen **Unter Verwendung von DHCP abrufen**.
8. Wenn Sie auf einem Netzwerk implementieren, das eine VLAN-ID erfordert, markieren Sie das VLAN-Kontrollkästchen und geben dann die VLAN-ID ein.

   Verwenden Sie für die VLAN-ID die Zahlen 1 bis 4094. Die VLAN-ID 0 wird für die Markierung der Priorität von Rahmen reserviert.
9. Wiederholen Sie die Schritte für alle bereitzustellenden Server oder aktivieren Sie das Kontrollkästchen **Einstellungen für alle ausgewählten Server übernehmen**.
10. Klicken Sie auf **Weiter**.

    Klicken Sie auf Bereitstellungsassistent Schritt 5: Verbindungsprofil, um die Aufgabe mit Schritt 5 fortzusetzen.

Bereitstellungsassistent Schritt 5: Verbindungsprofil

Verbindungsprofile dienen zum Herstellen eines Berechtigungsnachweis für Hosts, indem ihnen ein iDRAC- oder Host-Root-Berechtigungsnachweis zugeordnet wird. Im Fenster „Connection Profiles“ (Verbindungsprofile) können Sie:

- Ein Verbindungsprofil anzeigen oder bearbeiten
- Ein Verbindungsprofil löschen
- Die Liste der Verbindungsprofile aktualisieren, um die vCenter Host-Änderungen widerzuspiegeln

So erstellen Sie ein Verbindungsprofil:

1. Verbindungsprofile weisen Server automatisch zu Verbindungsprofilen zu, nachdem der Bereitstellungsauftrag abgeschlossen ist.

   Klicken Sie auf **Weiter**, nachdem Sie ein Verbindungsprofil ausgewählt haben.
2. Wählen Sie das Optionsfeld **Weisen Sie alle Server demselben Verbindungsprofil zu**, und wählen Sie ein Verbindungsprofil in der Dropdown-Liste aus, um alle Server zum gleichen bestehenden Profil zuzuweisen.
3. Klicken Sie auf **Neu**, um ein neues Profil zu erstellen, und klicken Sie dann auf **Anzeigen/Bearbeiten**, um das ausgewählte Profil anzuzeigen bzw. zu bearbeiten.
4. Klicken Sie auf **Anzeigen**, um die Einstellungen des ausgewählten Verbindungsprofils anzuzeigen.
5. Klicken Sie auf das Optionsfeld **Wählen Sie für jeden Server ein Verbindungsprofil aus** und wählen Sie dann für jeden Server ein Verbindungsprofil in der Dropdown-Liste aus.
6. Klicken Sie auf **Weiter**, nachdem Sie ein Verbindungsprofil ausgewählt haben.

   Klicken Sie auf Bereitstellungsassistent Schritt 6, um die Aufgabe mit Schritt 6 fortzusetzen.

Bereitstellungsassistent Schritt 6: Jobs planen

Ein Zeitplan legt die Planung eines Bereitstellungs-Jobs fest. Es gibt verschiedene Optionen, wenn der Bereitstellungs-Job ausgeführt werden soll: sofort, zu einer bestimmten Uhrzeit an einem bestimmten Datum und manuell starten.

So richten Sie einen Zeitplan ein:

1. Legen Sie das Datum und Uhrzeit der Ausführung des Bereitstellungs-Jobs fest:
   a. Klicken Sie auf **Zeitplan für die Bereitstellung der Server festlegen**.
   b. Verwenden Sie das Kalender-Bedienfeld, um ein Datum auszuwählen.
   c. Legen Sie die Uhrzeit fest:
      - Sofort: Klicken Sie auf **Server jetzt bereitstellen**.
      - Job später ausführen: Klicken Sie auf **Bereitstellungs-Job erstellen**.
      - Aussetzen: Mit dieser Option wird nur der Zeitplan modifiert. Alle anderen Bereitstellungsoptionen werden nicht geändert.
2. Geben Sie einen **Jobnamen** und eine **Jobbeschreibung** ein.
3. Klicken Sie auf **Fertigstellen**.
4. Jetzt, nachdem der Bereitstellungsassistent abgeschlossen ist, können Sie die Bereitstellungs-Jobs mithilfe der **Job-Warteschlange** verwalten.
5. Klicken Sie auf **Nicht-konforme Server**, um eine Liste aller nicht konformen Server anzuzeigen, für die zunächst eine Firmware-Aktualisierung durchgeführt werden muss.

Verwandte Aufgaben:

- Verwalten von Bereitstellungs-Jobs mit der Bereitstellungs-Jobwarteschlange

Die Job-Warteschlange

Die Job-Warteschlange verwaltet Jobs zur Serverbereitstellung und Erstellung von Bestandslisten. Dazu gehören:

- Anzeigen der übermittelten Jobs zur Serverbereitstellung.
- Aktualisieren von Bereitstellungs-Jobs oder Bestandsliste/Garantieverlauf-Warteschlangen.
- Planen eines Auftrags zum Erstellen einer Bestandsliste zum Aktualisieren der Dell Server-Attribute im aktuellen vCenter.
- Löschen der Einträge in der Bereitstellungs-Job-Warteschlange.
- Verwalten von Firmware-Aktualisierungen für Cluster und Datenzentren.



ANMERKUNG: Sie sollten das Erstellen einer Bestandsliste/Garantie mindestens einmal wöchentlich planen um sicherzustellen, dass die Bestandsliste/Garantie aktuelle Informationen enthält. Das Erstellen einer Bestandsliste/Garantie erfordert nur minimale Ressourcen und wirkt sich nicht negativ auf die Hostleistung aus.

Die Tasks auf dieser Seite umfassen:

- Verwalten von Bereitstellungs-Jobs mit der Bereitstellungs-Job-Warteschlange
- Ausführen von Bestandsaufnahme-Jobs
- Modifizieren eines Zeitplans zum Erstellen einer Bestandsliste
- Anzeige des Firmware-Aktualisierungs-Status für Cluster und Datenzentren.

Verwalten von Bereitstellungs-Jobs mit der Bereitstellungs-Jobs-Warteschlange

So verwalten Sie Bereitstellungs-Jobs mit der Bereitstellungs-Job-Warteschlange:

1. Wählen Sie im **Dell Management Center Job-Warteschlange Bereitstellungs-Jobs** aus.
2. Klicken Sie zum Aktualisieren der **Details zu Bereitstellungs-Jobs** auf **Aktualisieren**.
3. Klicken Sie auf **Details**, um das Dialogfeld „Details zu Bereitstellungs-Jobs“ anzuzeigen, dass ausführliche Informationen zu den Servern enthält, die in dem Bereitstellungs-Job enthalten sind. Hierzu gehören:
   - Service-Tag-Nummer
   - iDRAC-IP-Adresse
   - Serverstatus
   - Eventuell aufgetretene Warnmeldungen
   - Details zum Bereitstellungs-Job
   - Start- und Endzeit

   Um ausführliche Informationen zu jedem Element in der Tabelle des Dialogfeld anzuzeigen, halten Sie den Mauszeiger über das Element, bis ein Text mit zusätzlichen Informationen angezeigt wird.
4. Klicken Sie auf **Modifizieren**, um entweder einen ausgewählten Job anzuhalten oder einen aktualisierten Zeitplan einzugeben.
5. Klicken Sie auf **Abbrechen**, um den Bereitstellungs-Job abzubrechen.
6. Wenn die Bestätigungsaufforderung angezeigt wird, klicken Sie entweder auf **Job abbrechen**, um den Job abzubrechen, oder auf **Job nicht abbrechen**, um den Job weiter auszuführen.

   ANMERKUNG: Bereitstellungs-Jobs, die bereits ausgeführt werden, können nicht abgebrochen werden.
7. Klicken Sie auf **Job-Warteschlange säubern**, um das Fenster „Job-Warteschlange säubern“ anzuzeigen. Wählen Sie dann **Älter als Datum und Jobsstatus** und klicken Sie auf **Übernehmen**. Die ausgewählten Jobs werden aus der Warteschlange gelöscht.

Manuelles Hinzufügen eines Servers

Sie können einen Server, der vom Ermittlungsprozess nicht erkannt wurde, manuell hinzufügen. Nachdem der Server hinzugefügt wurde, erscheint er in der Liste der Server im Bereitstellungsassistenten.

1. Wählen Sie im Dell Management Center **Bereitstellung** und klicken Sie auf **Bereitstellungsassistent.**
2. Klicken Sie auf der Registerkarte **Server auswählen** auf **Server hinzufügen**.
3. Führen Sie im Dialogfeld **Server hinzufügen** die folgenden Schritte aus:
   a. Geben Sie die iDRAC-IP-Adresse in das Textfeld **iDRAC-IP-Adresse** ein.
   b. Geben Sie den Benutzernamen in das Textfeld **Benutzername** ein.
   c. Geben Sie das Kennwort in das Textfeld **Kennwort** ein.
4. Klicken Sie auf **Server hinzufügen**. Dieser Vorgang kann einige Minuten dauern.

Entfernen eines Bare-Metal-Servers

Sie können einen Server manuell entfernen, der automatisch ermittelt oder manuell hinzugefügt wurde.

1. Wählen Sie im Dell Management Center unter **Bereitstellung Bereitstellungsassistent.**
2. Klicken Sie auf der Registerkarte **Server auswählen** auf **Server entfernen**.
3. Aktivieren Sie das Kontrollkästchen neben dem zu entfernenden Server im Dialogfeld **Server entfernen**.
4. Klicken Sie auf **Ausgewählte Server entfernen**.

5. Zeigen Sie auf der Registerkarte **Server auswählen** die Server in der Tabelle an, um sicherzustellen, dass der gewünschte Server entfernt wurde.

6

Konsolenverwaltung

Die Verwaltung des OpenManage Integration for VMware vCenter und dessen virtueller Umgebung wird mithilfe zweier zusätzlicher Administrator-Portale erreicht:

- Web-basierte Administration Console
- Konsolenansicht für einen bestimmten Server (die Konsole der virtuellen Maschine des Geräts).

Über diese beiden Portale können globale Einstellungen für die Verwaltung von vCenter, Backup und Wiederherstellung der OpenManage Integration for VMware vCenter-Datenbank sowie Aktionen zum Zurücksetzen/Neustart eingegeben und für alle vCenter-Instanzen verwendet werden.

Web-basierte Administration Console

Die Web-basierte Administration Console bietet verschiedene Funktionen: vCenter-Serverregistrierung und -verwaltung, Verwaltung virtueller Geräte, globale vCenter-Alarmeinstellungen sowie Einstellungen für Backup und Wiederherstellung.

Verwalten von vCenter Serververbindungen

Im Fenster „vCenter Registration" in der Administration Console können Sie einen vCenter-Server registrieren, aktualisieren und eine Lizenz erwerben. Wenn Sie eine Demolizenz verwenden, wird der Link **Jetzt kaufen** angezeigt, über den Sie eine vollständige Produktversion erwerben können, um mehrere Hosts zu verwalten. In diesem Abschnitt können Sie auch einen Server modifieren, aktualisieren und die Registrierung aufheben.

Verwandte Aufgaben:

- Registrieren eines vCenter-Servers
  - Modifizieren der vCenter Administrator-Anmeldung
  - Aktualisieren der SSL-Zertifikate für registrierte Server
  - Deinstallieren von OpenManage Integration for VMware vCenter From vCenter
- Hochladen einer OpenManage Integration für VMware vCenter-Lizenz unter Verwendung der Administration Console

Registrieren eines vCenter-Servers

Sie können OpenManage Integration für VMware vCenter nach der Installation von OpenManage Integration for VMware vCenter registrieren. OpenManage Integration for VMware vCenter verwendet das Admin-Benutzerkonto für vCenter-Vorgänge. OpenManage Integration for VMware vCenter unterstützt 10 vCenters pro Gerät.

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung" zum Öffnen der Administrationskonsole.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.

3. Klicken Sie zum Registrieren eines neuen Servers im linken Fensterbereich auf **VCENTER REGISTRIERUNG** und dann auf **Neuen vCenter-Server registrieren**.
4. Führen Sie im Dialogfeld **Neues vCenter registrieren** unter **vCenter-Name** die folgenden Schritte aus:
   a. Geben Sie die vCenter-IP-Adresse oder ein FQDN des Hosts in das Textfeld **vCenter-Server-IP-Adresse oder Hostname** ein.
   b. Geben Sie optional eine Beschreibung in das Textfeld **Beschreibung** ein.
5. Unter **Admin-Benutzerkonto** führen Sie die folgenden Schritte aus:
   a. Geben Sie den Benutzernamen des Administrators in das Textfeld **Admin-Benutzername** ein.
   b. Geben Sie das Kennwort in das Textfeld **Kennwort** ein.
   c. Geben Sie das Kennwort zur Bestätigung in das Textfeld **Kennwort bestätigen** ein.
6. Klicken Sie auf **Registrieren**.

Anforderungen für OpenManage Integration for VMware vCenter

Die OpenManage Integration for VMware vCenter (OMIVV) erfordert Informationen von OpenManage auf Servern einer älteren Generation und neuere Plattformen sind darauf beschränkt, mit der Version von vSphere zu starten, die den neueren Chipsatz versteht. Daher gibt es Beschränkungen in Bezug auf die Version von vSphere, mit der eine bestimmte Version von OMIVV arbeitet.

ESXi-Versionen, die auf verwalteten Hosts unterstützt werden sollten:

ESX/ESXi-Version-Unterstützung	Plattform-Generation-Support				
	9G	10G	11G	12G	13G
v4.1 (ESX/ESXi)	J	J	J	N	N
v4.1 U1 (ESX/ESXi)	J	J	J	N	N
v4.1 U2 (ESX/ESXi)	J	J	J	J	N
v4.1 U3 (ESX/ESXi)	J	J	J	J	N
v5.0	J	J	J	J	N
v5.0 U1	J	J	J	J	N
v5.0 U2	J	J	J	J	N
v5.0 U3	J	J	J	J	N
v5.1	J	J	J	J	N
v5.1 U1	J	J	J	J	N
v5.1 U2	J	J	J	J	N
v5.5	N	j	J	J	N
v5.5 U1	N	N	N	N	J
v5.5 U2	N	N	N	J	J

vCenter sSupport

Derzeit ist die Unterstützung für v5.5 U1 nur mit Servern der 12. Generation über iDRAC mit Lifecycle Controller-Unterstützung verfügbar. OpenManage-Support für 5.5 U1 mit Servern der älteren Generation ist in Kürze zu erwarten. vSphere v5.5 U1 wird mit dem aktuellen Chipsatz nicht unterstützt, so wird es auf den Plattformen der 13. Generation auch nicht unterstützt.

Unterstützung für vSphere v5.5 U2

Mit der Unterstützung von iDRAC mit Lifecycle Controller 5.5 U2 wird vSphere für Plattformen der 12. und 13. Generation unterstützt.

Unterstützte vCenter Server-Versionen für Version 2.3

Die OpenManage Integration for VMware vCenter arbeitet mit jeder dieser vCenter Server-Versionen:

vCenter-Version	Desktop-Client-Support	Web-Client-Support
v5.0 U3	J	N
5.1 U2	J	N
v5.5	J	J
v5.5 U1	J	J
v5.5 U2	J	J

Mit jeder gegebenen vCenter-Version müssen die ESX / ESXi-Hosts, die es verwaltet, über eine gleiche oder niedrigere Version verfügen. Um eine vSphere v4.1- oder v5.0-Umgebung mit OMIVV zu verwalten, müssen Sie über eine vCenter-Mindestversion v5.0 U3 verfügen.

Modifizieren der vCenter Administrator-Anmeldung

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung" zum Öffnen der Administrationskonsole.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **VCENTER REGISTRIERUNG**. Die registrierten vCenter werden im rechten Fensterbereich angezeigt. Klicken Sie zum Öffnen des Fensters **Admin-Konto modifizieren** unter **Anmeldeinformationen** auf **Modifizieren**.
4. Geben Sie den **Benutzername** und das **Kennwort** für den vCenter Administrator ein, und bestätigen Sie das Kennwort unter **Kennwort bestätigen**.
5. Klicken Sie auf **Anwenden**, um das Kennwort zu ändern, oder klicken Sie auf **Abbrechen**, um den Vorgang abzubrechen.

Aktualisieren der SSL-Zertifikate für registrierte vCenter-Server

Wenn das SSL-Zertifikat auf einem vCenter-Server geändert wird, führen Sie die folgenden Schritte aus, um das neue Zertifikat für das OpenManage Integration for VMware vCenter zu importieren. DasOpenManage Integration for VMware vCenterr verwendet dieses Zertifikat, um sicherzustellen, dass der vCenter-Server mit dem richtigen vCenter-Server und nicht mit einem Nachahmer kommuniziert.

OpenManage Integration for VMware vCenter verwendet das openssl API zum Erstellen des Certificate Signing Request (CSR) unter Verwendung des RSA-Verschlüsselungsstandards mit einer 2048 Bitschlüssellänge. Das durch OpenManage Integration for VMware vCenter erstellte CRS erhält ein digital signiertes Zertifikat einer vertrauenswürdigen Zertifizierungsstelle. Das OpenManage Integration for VMware vCenter verwendet das digitale Zertifikat zum Aktivieren von SSL auf dem Webserver für eine sichere Kommunikation.

1. Starten Sie einen Web-Browser und geben Sie dann https://<ApplianceIPAdrdress> ein.
2. Klicken Sie im linken Fensterbereich auf **VCENTER REGISTRIERUNG**. Die registrierten vCenters werden im rechten Fensterbereich angezeigt. Zur Aktualisierung der Zertifikate klicken Sie auf **Aktualisieren**.

Deinstallieren des OpenManage Integration for VMware vCenter von VMware vCenter

Um das OpenManage Integration for VMware vCenter zu entfernen, müssen Sie die Registrierung des vCenter-Servers unter Verwendung der Administrationskonsole aufheben.

1. Starten Sie einen Webbrowser und geben Sie https://<ApplianceIPAdrdress> ein.
2. Heben Sie auf der Seite **vCenter Registrierung** unter der vCenter-Server-Tabelle die Registrierung der OpenManage Integration for VMware vCenter durch das Klicken auf **Registrierung aufheben** auf.

   Wenn Sie mit mehreren vCentern arbeiten, achten Sie darauf, das richtige auszuwählen.
3. Wenn Sie im Dialogfeld **vCenter-Registrierung aufheben** gefragt werden, ob Sie die Registrierung dieses Servers aufheben möchten, klicken Sie auf **Registrierung aufheben**.

Hochladen einer OpenManage Integration for VMware vCenter-Lizenz auf die Administrationskonsole

Um eine OpenManage Integration for VMware vCenter-Lizenz zum Administration Portal hochzuladen:

1. Starten Sie einen Webbrowser und geben Sie https://<ApplianceIPAddress> ein.
2. Klicken Sie im linken Fensterbereich auf **VCENTER REGISTRIERUNG**. Die registrierten vCenter werden im rechten Fensterbereich angezeigt. Klicken Sie zum Anzeigen des Dialogfelds „Lizenz hochladen" auf **Lizenz hochladen**.
3. Klicken Sie auf die Schaltfläche **Durchsuchen**, um das Verzeichnis mit der Lizenzdatei zu suchen, und klicken Sie dann auf **Hochladen**.

   
   ANMERKUNG: Wenn die Lizenzdatei geändert oder anderweitig bearbeitet wird, betrachtet sie das Gerät als beschädigt und die Datei wird nicht akzeptiert.

Verwalten des virtuellen Geräts

Das Verwalten des virtuellen Geräts beinhaltet das OpenManage Integration for VMware vCenter-Netzwerk, die -Version, die -NTP- und HTTPS-Informationen und ermöglicht einem Administrator:

- Neustarten des virtuellen Geräts
- Aktualisieren des virtuellen Geräts und Konfigurieren eines Speicherorts für die Repository-Aktualisierung
- Erzeugen eines Fehlerbehebungspakets, das Anmeldeinformationen des Geräts enthält.
- Einrichten der Network Time Protocol (NTP)-Einstellungen
- Hochladen und Verwalten von HTTPS-Zertifikaten

Verwandte Aufgaben:

- Neustarten des virtuellen Geräts
- Aktualisieren eines Repository-Speicherort und eines Geräts
- Herunterladen des Bündels für Fehlerbehebung
- Einrichten der NTP-Server

Neustarten des virtuellen Geräts

So starten Sie das virtuelle Gerät neu:



ANMERKUNG: Das Neustarten des virtuellen Gerät meldet Sie von der Administration Console ab und das OpenManage Integration for VMware vCenter ist nicht mehr verfügbar, bis das virtuelle Gerät und seine Dienste aktiv sind.

1. Starten Sie einen Webbrowser und geben Sie https://<ApplianceIPAddress> ein.
2. Klicken Sie im linken Fensterbereich auf **GERÄTEVERWALTUNG**.
3. Zu Neustart des OpenManage Integration for VMware vCenter klicken Sie auf **Neustarten des virtuellen Geräts**.
4. Klicken Sie im Dialogfeld **Virtuelles Gerät neustarten** auf **Anwenden**, um das virtuelle Gerät neu zu starten, oder auf **Abbrechen**, um den Vorgang abzubrechen.

Aktualisieren eines Repository-Speicherorts und virtuellen Geräts

Führen Sie vor dem Aktualisieren des virtuelle Geräts ein Backup aus, um sicherzustellen, dass alle Daten geschützt sind.

1. Starten Sie einen Webbrowser und geben Sie https://<ApplianceIPAddress> ein.
2. Klicken Sie im linken Fensterbereich auf **GERÄTEVERWALTUNG**.
3. Klicken Sie neben „Geräteaktualisierung" auf **Bearbeiten**.
4. Im Fenster **Geräteaktualisierung** geben Sie die **Repository-Standort URL** ein und klicken Sie auf **Anwenden**.

   ANMERKUNG: Wenn sicher der Aktualisierungsspeicherort in einem externen Netzwerk befindet (z. B. der Dell FTP-Site), muss ein Proxyserver im Bereich „HTTP Proxy" angegeben werden.

Aktualisieren der Softwareversion des virtuellen Geräts

Erstellen Sie vor der Softwareaktualisierung ein Backup der Daten auf dem virtuellen Gerät, um einen möglichen Datenverlust vermeiden.

1. Starten Sie einen Web-Browser und geben Sie dann https://<ApplianceIPAddress> ein.
2. Klicken Sie im linken Fensterbereich auf **GERÄTEWARTUNG**.
3. Klicken Sie zum Aktualisieren der Softwareversion des virtuellen Geräts unter **Geräteaktualisierung** auf **Virtuelles Gerät aktualisieren**.
4. Im Dialogfeld **Gerät aktualisieren** werden die aktuelle und die verfügbare Versionen aufgeführt. Klicken Sie auf **Aktualisieren**, um die Aktualisierung zu beginnen.
5. Das System wird gesperrt und in den Wartungsmodus versetzt. Nachdem die Aktualisierung abgeschlossen ist, zeigt die Seite „Gerät" die neu installierte Version an.

Herunterladen des Fehlerbehebungsbündels

Verwenden Sie diese Informationen bei einer Fehlerbehebung oder senden Sie sie an den technischen Support.

1. Starten Sie einen Web-Browser und geben Sie dann https://<ApplianceIPAddress> ein.
2. Klicken Sie im linken Fensterbereich auf **GERÄTEVERWALTUNG**.
3. Klicken Sie auf **Bündel für Fehlerbehebung erstellen**, um das Dialogfeld „Bündel für Fehlerbehebung" anzuzeigen.
4. Klicken Sie auf den Link **Bündel für Fehlerbehebung herunterladen**, um die Zip-Datei mit den Anmeldeinformationen für das virtuelle Gerät entweder zu öffnen oder zu speichern.
5. Klicken Sie zum Beenden auf **Schließen**.

Einrichten des HTTP-Proxy

Sie können die HTTP-Proxy-Einstellungen entweder in der Administrator Console oder in der Dell Management Console einrichten.

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung" zum Öffnen der Administrationskonsole.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **GERÄTEVERWALTUNG**.
4. Scrollen Sie auf der Seite **Geräteverwaltung** bis zu **HTTP-Proxy-Einstellungen** und klicken Sie dann auf **Bearbeiten**.
5. Führen Sie auf der Seite **Bearbeiten** die folgenden Schritte aus:
   a. Wählen Sie neben **HTTP-Proxy-Einstellungen verwenden** die Option **Aktivieren**.
   b. Geben Sie die Proxyserver-Adresse in das Textfeld **Proxyserver-Adresse** ein.
   c. Geben Sie den Proxyserver-Port in das Textfeld **Proxyserver-Schnittstelle** ein.
   d. Wählen Sie neben **Proxy-Anmeldeinformationsnachweis verwenden** die Option **Ja**, um die Proxy-Anmeldeinformationen zu verwenden.
   e. Wenn Sie ie Anmeldeinformationen verwenden, geben Sie den Benutzernamen in das Textfeld **Benutzername** ein.
   f. Geben Sie das Kennwort in das Textfeld **Kennwort** ein.
6. Klicken Sie auf **Anwenden**.

Einrichten der NTP-Server

Verwenden Sie das Network Time Protocol (NTP) zum Synchronisieren der Uhren der virtuellen Geräte mit der Uhr eines NTP-Servers.

1. Verwenden Sie den Link in der Registerkarte „Zusammenfassung" in OpenManage Integration for VMware vCenter, um die Administration Console zu öffnen.
2. Geben Sie Ihr Kennwort in dem Anmeldedialogfenster ein.
3. Klicken Sie im linken Fensterbereich auf **GERÄTEVERWALTUNG**.
4. Klicken Sie auf **Für NTP bearbeiten**.
5. Aktivieren Sie das Kontrollkästchen **Aktiviert**. Geben Sie den **Hostnamen** oder die **IP-Adresse** für einen **bevorzugten** und einen **sekundären NTP-Server** ein und klicken Sie auf **Anwenden**.
6. Klicken Sie auf **Abbrechen**, um den Vorgang abzubrechen.

Erzeugen einer Zertifikatsignierungsanforderung



ANMERKUNG: Sie müssen das Zertifikat vor der Registrierung des OpenManage Integration for VMware vCenter mit vCenter hochladen.

Das Erzeugen einer Zertifikatsignierungsanforderung verhindert, dass Zertifikate mit zuvor erstellten CSR auf das Gerät hochgeladen werden.

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung" zum Öffnen der Administrationskonsole.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **GERÄTEVERWALTUNG**.
4. Klicken Sie auf **Zertifikatsignierungsanforderung für HTTPS-Zertifikate erzeugen**. Eine Meldung zeigt an, dass wenn eine neue Anforderung erzeugt wird, mit dem vorherigen CSR erzeugte Zertifikate nicht mehr auf das Gerät hochgeladen werden. Klicken Sie zum Fortsetzen der Anforderung auf **Weiter**, oder klicken Sie auf **Abbrechen**, um den Vorgang abzubrechen.

5. Geben Sie den **Allgemeinen Namen,Name der Organisation**, **Organisationseinheit**, **Standort**, **Name des Bundeslands/der Provinz**, **Land** und **E-Mail-Adresse** für die Anforderung ein. Klicken Sie dann auf **Fortsetzen**.
6. Klicken Sie auf **Herunterladen**, dann speichern Sie das resultierende HTTPS-Zertifikat an einem zugänglichen Speicherort.

Hochladen eines HTTPS-Zertifikats

HTTPS-Zertifikate werden für die sichere Kommunikation zwischen dem virtuellen Gerät und Hostsystemen verwendet. Um diese sichere Kommunikation einzurichten, muss eine Zertifikatssignierungsanfrage an eine Zertifizierungsstelle gesendet werden, dann wird das resultierende Zertifikat mithilfe der Administration Console hochgeladen. Darüber hinaus gibt es ein selbst-signiertes Standardzertifikat, das für die sichere Kommunikation verwendet werden kann; dieses Zertifikat ist bei jeder Installation einmalig.

 **ANMERKUNG:** Sie können entweder Microsoft Internet Explorer, Firefox oder Chrome verwenden, um Zertifikate hochzuladen.

1. Verwenden Sie den Link in OpenManage Integration for VMware vCenter in der Registerkarte „Zusammenfassung“ zum Öffnen der Administrationskonsole.
2. Geben Sie im Anmelde-Dialogfeld Ihr Kennwort ein.
3. Klicken Sie im linken Fensterbereich auf **GERÄTEVERWALTUNG**.
4. Klicken Sie auf **Zertifikat für HTTPS-Zertifikate hochladen**.
5. Klicken Sie im Dialogfeld **Zertifikate hochladen** auf **OK**.
6. Klicken Sie zum Auswählen des gewünschten Zertifikats auf **Durchsuchen** und dann auf **Hochladen**.
7. Klicken Sie auf **Abbrechen**, wenn Sie das Hochladen abbrechen müssen.

    **ANMERKUNG:** Das Zertifikat muss im PEM-Format vorliegen.

Wiederherstellen des standardmäßigen HTTPS-Zertifikats

1. Verwenden Sie den Link in der Registerkarte „Zusammenfassung“ in OpenManage Integration for VMware vCenter, um die Administration Console zu öffnen.
2. Geben Sie Ihr Kennwort in dem Anmeldedialogfenster ein.
3. Klicken Sie im linken Fensterbereich auf **GERÄTEVERWALTUNG**.
4. Klicken Sie auf **Standardmäßiges Zertifikat für HTTPS-Zertifikate wiederherstellen**.
5. Klicken Sie im Dialogfeld „Standardmäßiges Zertifikat wiederherstellen“ auf **Anwenden**.

Einrichten globaler Alarme

Mit der Alarmverwaltung können Sie globale Einstellungen, wie Alarme für alle vCenter-Instanzen gespeichert werden, festlegen.

1. Verwenden Sie den Link in der Registerkarte „Zusammenfassung“ in OpenManage Integration for VMware vCenter, um die Administration Console zu öffnen.
2. Geben Sie Ihr Kennwort in dem Anmeldedialogfenster ein.
3. Klicken Sie im linken Fensterbereich auf **ALARMVERWALTUNG**. Klicken Sie auf **Bearbeiten**, um neue vCenter-Alarmeinstellungen festzulegen.
4. Geben Sie numerische Werte für die folgenden Elemente ein:

   - Maximale Anzahl an Alarmen
   - Anzahl an Tagen, über die Alarme beibehalten werden sollen
   - Timeout für duplizierte Alarme (Sekunden)
5. Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern, oder klicken Sie auf **Abbrechen**, um die Änderungen zu verwerfen.

Verwalten von Backups und Wiederherstellungen

Die Verwaltung von Backups und Wiederherstellungen erfolgt über die Administrator Console. Die Tasks auf dieser Seite umfassen:

- Konfigurieren von Backup und Wiederherstellung
- Planen von automatischen Backups
- Durchführen eines sofortigen Backups
- Wiederherstellen der Datenbank aus einem Backup

Konfigurieren von Backup und Wiederherstellung

Die Funktionen für das Backup und die Wiederherstellung sichern die Datenbank des OpenManage Integration for VMware vCenter an einem remoten Speicherort, von dem aus sie zu einem späteren Zeitpunkt wieder hergestellt werden kann. Wir empfehlen, das Sie zum Schutz gegen Datenverlust automatische Backups planen. Nach diesem Verfahren müssen Sie einen Backup-Zeitplan konfigurieren.

So konfigurieren Sie Backup und Wiederherstellung:

1. Starten Sie einen Webbrowser und geben Sie https://<ApplianceIPAddress> ein.
2. Klicken Sie im linken Fensterbereich auf **BACKUP UND WIEDERHERSTELLUNG**.
3. Klicken Sie auf **Bearbeiten**, um die aktuellen Einstellungen für Backup und Wiederherstellung zu bearbeiten.
4. Führen Sie auf der Seite **Einstellungen und Details** die folgenden Schritte aus:
   a. Geben Sie den Pfad zu den gesicherten Dateien in das Textfeld **Speicherort des Backups** ein.
   b. Geben Sie den Benutzernamen in das Textfeld **Benutzername** ein.
   c. Geben Sie das Kennwort in das Textfeld **Kennwort** ein.
   d. Geben Sie das Verschlüsselungskennwort in das Textfeld **Kennwort für die Verschlüsselung von Backups** ein.

      Das Verschlüsselungskennwort darf alphanumerische und die folgenden Sonderzeichen enthalten: !@#$%*. Es gibt keine Längenbeschränkung.
   e. Geben Sie das Verschlüsselungskennwort erneut in das Textfeld **Kennwort bestätigen** ein.
5. Klicken Sie auf **Anwenden**, um diese Einstellungen zu speichern.
6. Konfigurieren Sie den Backup-Zeitplan. Weitere Informationen finden Sie unter Planen von automatischen Backups.

Planen von automatischen Backups

Dies ist der zweite Teil der Konfiguration von Backup und Wiederherstellung. Ausführliche Informationen zum Konfigurieren des Backup-Speicherorts und des Berechtigungsnachweises finden Sie unter Konfigurieren von Backup und Wiederherstellung.
So konfigurieren Sie ein automatisches Backup:

1. Starten Sie einen Webbrowser und geben Sie https://<ApplianceIPAddress> ein.
2. Klicken Sie im linken Fensterbereich auf **BACKUP UND WIEDERHERSTELLUNG**.
3. Klicken Sie auf **Bearbeiten Automatisch geplanter Backup**, um die Einstellungen für Backup und Wiederherstellung zu ändern. Das Feld wird aktiviert.
4. Klicken Sie auf **Aktiviert**, um Backups zu aktivieren.
5. Aktivieren Sie die Kontrollkästchen der Tage, an denen ein Backup durchgeführt werden soll .
6. Geben Sie die Zeit in dem Format HH:MM in das Textfeld **Uhrzeit für Backup (24 Stunden Uhrzeitformat, HH:mm)** ein.

   Das Feld **Nächster Backup** wird mit dem Datum und der Uhrzeit für den nächsten geplanten Backup ausgefüllt.

7. Klicken Sie auf **Anwenden**.

Durchführen eines sofortigen Backups

So starten Sie ein sofortiges Backup:

1. Starten Sie einen Webbrowser und geben Sie https://<ApplianceIPAddress> ein.
2. Klicken Sie im linken Fensterbereich auf **BACKUP UND WIEDERHERSTELLUNG**.
3. Klicken Sie auf **Jetzt sichern**.
4. Aktivieren Sie im Dialogfeld **Jetzt sichern** das entsprechende Kontrollkästchen, um den angezeigten Speicherort und das Verschlüsselungskennwort zu verwenden.
5. Geben Sie einen **Speicherort für das Backup**, einen **Benutzernamen**, ein **Kennwort** und das **Verschlüsselungskennwort** ein.

   Das Verschlüsselungskennwort darf alphanumerische und die folgenden Sonderzeichen enthalten: !@#$%*. Es gibt keine Längenbeschränkung.
6. Klicken Sie auf **Sichern**.

Wiederherstellen der Datenbank aus einem Backup

ANMERKUNG: Bei einer Wiederherstellung wird das virtuelle Geräte nach Abschluss der Wiederherstellung neu gestartet wird.

So stellen Sie eine Datenbank aus einem Backup wieder her:

1. Starten Sie einen Webbrowser und geben Sie https://<ApplianceIPAddress> ein.
2. Klicken Sie im linken Fensterbereich auf **BACKUP UND WIEDERHERSTELLUNG**. Die aktuellen Einstellungen für das Backup und die Wiederherstellung werden angezeigt.
3. Klicken Sie auf **Jetzt wiederherstellen**.
4. Geben Sie einen **Dateispeicherort (CIFS/NFS-Format)** in das Dialogfeld „Jetzt wiederherstellen" ein.
5. Geben Sie den **Benutzernamen**, das **Kennwort** und das **Verschlüsselungskennwort** für die Backup-Datei ein.

   Das Verschlüsselungskennwort darf alphanumerische und die folgenden Sonderzeichen enthalten: !@#$%*. Es gibt keine Längenbeschränkung.
6. Klicken Sie auf **Anwenden** , um Ihre Änderungen zu speichern.

   Das Gerät wird neu gebootet oder startet neu, nachdem Sie auf „Anwenden" geklickt haben.

Grundlegendes zur vSphere Client-Konsole

Die **Konsole** befindet sich innerhalb des vSphere-Clients auf einer virtuellen Maschine. Die **Konsole** arbeitet Hand in Hand mit der Administrationskonsole. Die Konsole ermöglicht die Ausführung folgender Aufgaben:

- Konfiguration von Netzwerkeinstellungen
- Ändern des Kennworts des virtuellen Geräts
- Einstellen der lokalen Uhrzeit
- Neustart des virtuellen Geräts
- Zurücksetzen des virtuellen Geräts auf die werkseitigen Einstellungen
- Aktualisieren der Konsole
- Option Abmelden

Verwenden Sie die Pfeiltasten, um nach oben oder unten zu navigieren. Wenn Sie die gewünschte Option einmal ausgewählt haben, drücken Sie die **<EINGABETASTE>**. Wenn Sie auf den **Konsole**nbildschirm zugreifen, übernimmt der VMware vSphere-Client die Kontrolle Ihres Cursors. Um dieser Kontrolle zu entgehen, drücken Sie **<STRG> + <ALT>**.

Konfigurieren der Netzwerkeinstellungen

Die Netzwerkeinstellungen werden im vSphere-Client auf der Registerkarte **Konsole** eingerichtet.
So konfigurieren Sie die Netzwerkeinstellungen:

1. Wählen Sie in **vSphere Web Client** die OpenManage Integration for VMware vCenter, und klicken Sie dann auf die Registerkarte **Konsole.**
2. Wählen Sie im Fenster **Konsole** die Option **Netzwerk konfigurieren** und drücken Sie die **<EINGABETASTE>**.
3. Geben Sie die gewünschten Netzwerkeinstellungen unter **Geräte bearbeiten** oder unter **DNS bearbeiten** ein und klicken Sie auf **Speichern und Beenden**. Klicken Sie auf **Beenden**, um die Änderungen zu verwerfen.

Ändern des Kennworts des virtuellen Geräts

Das Kennwort des virtuellen Geräts wird im vSphere-Client auf der Registerkarte **Konsole** geändert.
So ändern Sie das Kennwort des virtuellen Geräts:

1. Wählen Sie in vSphere Web Client die virtuelle OpenManage Integration for VMware vCenter-Maschine und klicken Sie dann auf die Registerkarte **Konsole**
2. Wählen Sie auf der Registerkarte **Konsole** die Option **Admin-Kennwort ändern** mit den Pfeiltasten aus und drücken Sie die **<EINGABETASTE>**.
3. Geben Sie das **Aktuelle Admin-Kennwort** ein und drücken Sie die **<EINGABETASTE>**.

   Admin-Kennwörter müssen ein Sonderzeichen, eine Zahl, einen Großbuchstaben, einen Kleinbuchstaben und mindestens acht Buchstaben umfassen.
4. Geben Sie ein neues Kennwort unter **Neues Admin-Kennwort eingeben** ein und drücken Sie die **<EINGABETASTE>**.
5. Geben Sie das neue Kennwort erneut in das Textfeld **Admin-Kennwort bestätigen** ein und drücken Sie die **<EINGABETASTE>**. Das Administrator-Kennwort wird geändert.

Einstellen der lokalen Uhrzeit

So stellen Sie die lokale Uhrzeit ein:



ANMERKUNG: Sie können nur die Zeitzone und nicht die aktuelle Uhrzeit oder das Datum bearbeiten.

1. Wählen Sie im **vSphere Client** die OpenManage Integration for VMware vCenter virtuelle Maschine aus und klicken Sie dann auf die Registerkarte **Konsole**.
2. Wählen Sie **Zeitzone einstellen** und drücken Sie die **<EINGABETASTE>**.
3. Wählen Sie im Fenster **Auswahl der Zeitzone** die gewünschte Zeitzone aus und klicken Sie auf **OK**. Klicken Sie auf **Abbrechen**, um den Vorgang abzubrechen, ohne die Zeitzone zu ändern. Die Zeitzone wird aktualisiert.

Neustarten des virtuellen Geräts

So starten Sie das virtuelle Gerät neu:

1. Wählen Sie im **vSphere Client** die OpenManage Integration for VMware vCenter virtuelle Maschine aus und klicken Sie dann auf die Registerkarte **Konsole**.
2. Wählen Sie **Dieses virtuelle Gerät neustarten** und drücken Sie die **<EINGABETASTE>**.

3. Die folgende Meldung wird angezeigt:

```
If there are any processes running on this appliance they will be
terminated by this action. Are you sure you wish to do this?
```

4. Drücken Sie **y** (j), um den Neustart fortzusetzen, oder drücken Sie **n**, um den Vorgang abzubrechen. Das Gerät wird neu gestartet.

Zurücksetzen des virtuellen Geräts auf die werkseitigen Einstellungen

So setzen Sie das virtuelle Gerät auf die werkseitigen Einstellungen zurück:

1. Wählen Sie in **vSphere Web Client** die virtuelle OpenManage Integration for VMware vCenter-Maschine und klicken Sie dann auf das Register **Konsole**
2. Wählen Sie **Dieses virtuelle Gerät auf die werkseitigen Einstellungen zurücksetzen** und drücken Sie die **<EINGABETASTE>**.
3. Die folgende Meldung wird angezeigt:

```
This operation is completely Irreversible if you continue you will
completely reset *this* appliance to its original settings. All changes you
have made to this appliance will be Lost. Are you sure you wish to Reset
this Appliance to Factory Settings?
```

4. Geben Sie **y** zum Reset oder **n** zum Abbrechen ein.

   Das Gerät wird auf die ursprünglichen werksseitigen Standardeinstellungen zurückgesetzt und alle anderen Einstellungen und gespeicherten Daten gehen verloren.

    **ANMERKUNG:** Wenn das virtuelle Gerät auf die werkseitigen Einstellungen zurückgesetzt wird, werden alle Aktualisierungen an der Netzwerkkonfiguration beibehalten; diese Einstellungen werden nicht zurückgesetzt.

Aktualisieren der Konsolenansicht

Wählen Sie **Aktualisieren**, um die Konsolenansicht zu aktualisieren, und drücken Sie die **<EINGABETASTE>**.

Schreibgeschützte Benutzerrolle

Es gibt eine Benutzerrolle ohne Rechte mit der Bezeichnung „Nur-Lesen“ mit Shell-Zugriff für Diagnosezwecke. Der Nur-Lesen-Benutzer verfügt über eingeschränkte Rechte zum Ausführen der eingehängten Geräte. Das Kennwort des Nur-Lesen-Benutzers entspricht dem des Administrators.

Migrationspfad zur Migration von 1.6/1.7 auf 2.3

Es gibt keine Unterstützung für die RPM-Aktualisierung von Version 1.7. oder früher auf diese Version. Sie können mithilfe des Backup- und Wiederherstellungspfads eine Aktualisierung von einer älteren Version (1.6 oder 1.7) auf Version 2.3 durchführen. Der Migrationspfad wird ebenfalls nur ausgehend von Version 1.6 oder 1.7 unterstützt. Wenn Sie eine Version vor Version 1.6 ausführen, müssen Sie eine Erweiterung Ihres Geräts auf die unterstützte Version durchführen, bevor Sie mit der Migration auf OpenManage Integration for VMware vCenter Version 2.3 beginnen.

Führen Sie die folgenden Schritte durch, um von einer älteren Version auf OpenManage Integration for VMware vCenter Version 2.3 zu migrieren:

1. Erstellen Sie eine Sicherungskopie der Datenbank der älteren Versionen. Weitere Informationen finden Sie in den Abschnitten **Managing Backup and Restore** (Verwalten von Sicherung und Wiederherstellung) in diesem Handbuch.
2. Fahren Sie die älteren Geräte des vCenters herunter.

ANMERKUNG: Heben Sie nicht die Registrierung des vCenter-Plugins auf. Das Aufheben der vCenter-Plugin-Registrierung entfernt alle auf dem Plugin durch vCenter registrierten Alarme und alle benutzerdefinierten Vorgänge, wie Maßnahmen auf dem vCenter. Weitere Informationen finden Sie im Abschnitt **Wiederherstellung nach dem Aufheben der Registrierung des älteren Plugins nach einem Backup** in diesem Handbuch, sollten Sie das Aufheben der Registrierung des Plugins nach einem Backup bereits vorgenommen haben.

3. Stellen Sie die neue OpenManage Integration Version 2.3 OVF bereit. Weitere Informationen zur Bereitstellung des OVFs finden Sie im Abschnitt **Bereitstellen des OpenManage Integration for VMware vCenter OVF unter Verwendung des vSphere Clients** in diesem Handbuch.
4. Starten Sie das OpenManage Integration Version 2.3-Gerät.
5. Stellen Sie das Netzwerk, die Zeitzone usw. auf dem Gerät ein. Es wird empfohlen, dass das neue OpenManage Integration Version 2.3-Gerät dieselbe IP-Adresse, wie das alte Gerät hat. Weitere Informationen zum Einstellen der Netzwerkdetails finden Sie im Abschnitt **Registrierung des OpenManage Integration for VMware vCenter und Importieren der Lizenzdatei** in diesem Handbuch.
6. Wiederherstellen der Datenbank auf dem neuen Gerät. Weitere Informationen finden Sie im Abschnitt **Wiederherstellen der Datenbank mithilfe eines Backups** in diesem Handbuch.
7. Laden Sie die neue Lizenzdatei hoch. Weitere Informationen finden Sie im Abschnitt **Registrieren von OpenManage Integration for VMware vCenter und Importieren der Lizenzdatei** im **OpenManage Integration Version 2.3 Quick Install Guide** (Schnellinstallationsanleitung).
8. Überprüfen des Geräts. Weitere Informationen zum Sicherstellen, dass die Datenbankmigration erfolgreich war, finden Sie im Abschnitt **Überprüfung der Installation** in diesem Handbuch.
9. Führen Sie die Bestandsaufnahme auf allen registrierten vCentern aus.



ANMERKUNG:

Es wird empfohlen, dass Sie die Bestandsaufnahme auf allen durch das Plugin verwalteten Hosts nach der Aktualisierung durchführen. Weitere Informationen zum Ausführen der Bestandsaufnahme nach Bedarf finden Sie im Abschnitt **Ausführen von Bestandsaufnahme-Jobs**.

Sollte die IP-Adresse des neuen OpenManage Integration Version 2.3-Geräts von der des alten Geräts abweichen, muss das Trap-Ziel der SNMP-Traps so konfiguriert werden, dass es auf das neue Gerät verweist. Bei Servern ab der 12. Generation wird das Problem durch Ausführen der Bestandsaufnahme auf diesen Hosts behoben. Für alle Hosts der 11. oder einer noch älteren Generation, die früher konform waren, wird die IP-Adresse als nicht konform angezeigt und die Konfiguration von OMSA ist erforderlich. Weitere Informationen zum Reparieren der Host-Übereinstimmung finden Sie im Abschnitt **Ausführen des Assistenten zum Reparieren von nicht konformen vSphere-Hosts** in diesem Handbuch.

7

Troubleshooting

Verwenden Sie diesen Abschnitt, um Antworten auf Fragen zur Fehlerbeseitigung zu finden. Dieser Abschnitt umfasst:

- Häufig gestellte Fragen (FAQs)
- Probleme bei der Bare-Metal-Bereitstellung
- Kontaktaufnahme mit Dell
- Zugehörige Produktinformationen

Häufig gestellte Fragen (FAQs)

In diesem Abschnitt werden einige allgemeine Fragen und Lösungen beschrieben.

Die Verwendung von OpenManage Integration for VMware vCenter zum Aktualisieren einer Intel-Netzwerkkarte mit der Firmwareversion 13.5.2 wird nicht unterstützt.

Es gibt ein bekanntes Problem mit der 12. Generation der Dell PowerEdge-Server und einigen Intel-Netzwerkkarten mit der Firmwareversion 13.5.2. Das Aktualisieren einiger Intel-Netzwerkkartenmodelle mit dieser Firmwareversion schlägt fehl, wenn die Firmware-Aktualisierung mithilfe von Lifecycle Controller durchgeführt wird. Kunden, die diese Firmwareversion verwenden, müssen die Netzwerktreibersoftware mithilfe eines Betriebssystems aktualisieren. Wenn die Firmwareversion der Intel-Netzwerkkarte eine andere ist als 13.5.2, können Sie die Aktualisierung mithilfe von OpenManage Integration for VMware vCenter durchführen. Weitere Informationen finden Sie unter http://en.community.dell.com/techcenter/b/techcenter/archive/2013/03/20/intel-network-controller-card-with-v13-5-2-firmware-cannot-be-upgraded-using-lifecycle-controller-to-v13-5-6.aspx.



ANMERKUNG: Hinweis: Wählen Sie bei der Anwendung einer Firmware-Aktualisierung vom Typ 1:n keine Intel-Netzwerkadapter der Version 13.5.2 aus. Anderenfalls schlägt die Aktualisierung fehl und die Aktualisierungsaufgabe für die verbleibenden Server wird gestoppt.

Beim Versuch einer Firmware-Aktualisierung mit einer ungültigen DUP fällt der Hardware-Job-Status auf der vCenter-Konsole stundenlang weder aus noch weist er eine Zeitüberschreitung auf. Der Job-Status in LC zeigt aber dennoch „FEHLGESCHLAGEN“ an. Warum ist das so?

Wenn die ungültige DUP für die Firmware-Aktualisierung abgerufen wird, bleibt der Status der Aufgabe im vCenter-Konsolen-Fenster auf „In Progress“ (In Bearbeitung), die Meldung wird jedoch auf die Ursache des Fehlers geändert. Dies ist ein bekannter Fehler von VMWare und wird in zukünftigen Versionen von VMware vCenter behoben.

Lösung: Die Aufgabe muss manuell abgebrochen werden.

Betroffene Version: Alle

Administration-Portal zeigt immer noch den nicht erreichbaren Aktualisierungs-Repository-Speicherort an.

Wenn der vom Benutzer bereitgestellte Aktualisierungs-Repository-Pfad nicht erreichbar ist, wird die Fehlermeldung „Failed: Fehler beim Herstellen einer Verbindung mit der URL...“ oben in der System-Aktualisierungsansicht angezeigt, jedoch wird der Aktualisierungs-Repository-Pfad nicht auf den Wert vor der Aktualisierung zurückgesetzt.

Lösung: Gehen Sie von dieser Seite auf eine andere Seite und stellen Sie sicher, dass die Seite aktualisiert wird.

Betroffene Version: Alle

Warum werden die DNS-Konfigurationseinstellungen nach dem Neustart des Geräts auf die ursprünglichen Einstellungen zurückgesetzt, wenn für die Geräte-IP DHCP verwendet und die DNS-Einstellungen überschrieben werden?

Es ist ein bekannter Fehler, dass statisch zugewiesene DNS-Einstellungen durch die Werte aus dem DHCP ersetzt werden. Das kann vorkommen, wenn DHCP zum Bezug der IP-Einstellungen verwendet wird und DNS-Werte statisch zugewiesen werden. Wenn der DHCP-Lease verlängert oder das System neu gestartet wird, werden die zugewiesenen DNS-Einstellungen entfernt. Lösung: IP-Einstellungen statisch zuweisen, wenn sich die DNS-Servereinstellungen von DHCP unterscheiden.

Betroffene Version: Alle

Warum ist mein System bei der Durchführung einer 1:n-Firmware-Aktualisierung nicht in den Wartungsmodus gewechselt?

Bei einigen Firmware-Aktualisierungen muss der Host nicht neu gestartet werden. In dem Fall wird die Firmware-Aktualisierung durchgeführt, ohne dass der Host in den Wartungsmodus wechselt.

Selbst wenn mein Repository über Bundles für das ausgewählte 11G-System verfügt, zeigt die Firmware-Aktualisierung, dass ich über keine Bundles für eine Firmware-Aktualisierung verfüge, an.

Als ich im Sperrmodus einen Host zum Verbindungsprofil hinzugefügt habe, wurde eine Bestandsaufnahme gestartet, die jedoch mit der Meldung „Es wurde kein Remote Access Controller gefunden, oder auf diesem Host wird keine Bestandsaufnahme unterstützt“ fehlschlug. Die Bestandsaufnahme sollte jedoch für einen Host im Sperrmodus funktionieren, oder?

Wenn Sie den Host in den Sperrmodus versetzen oder den Sperrmodus von einem Host entfernen, müssen Sie mindestens 30 Minuten warten, bevor Sie mit dem nächsten Vorgang in der Option „Wenn ich einen 11G-Host für eine Firmware-Aktualisierung auswähle“ durchführen können. Der Assistent zur Firmware-Aktualisierung zeigt keine Bundles an, selbst, wenn das Repository Bundles für das System bereitgestellt hat. Dies tritt ein, da der 11G-Host eventuell nicht dafür konfiguriert ist, dass OMSA Traps zu OpenManage Integration sendet.

Lösung: Stellen Sie sicher, dass der Host mit dem Host-Compliance-Bildschirm des OpenManage Integration Desktop-Clients kompatibel ist. Wenn sie nicht konform sind, verwenden Sie die Option „Host-Konformitätprobleme beheben“, um die Konformität herzustellen.

Betroffene Versionen: 2.2 und 2.3

Warum schlägt die ESX/ESXi-Bereitstellung auf Servern mit PERC S300-Startcontroller fehl?

Bereitstellungen des OpenManage Integration for VMware vCenter mit unterschiedlichen ESX/ESXi-Versionen schlagen auf Dell PowerEdge-Servern mit PERC S300-Startcontroller fehl. Die benutzerdefinierten Dell ESX/ESXi-Betriebssysteme verfügen nicht über den Treiber für den PERC S300-Startcontroller, was dazu führt, dass der Startcontroller/die HDD bei der Betriebssysteminstallation nicht erkannt wird. Server mit PERC S300-Startcontroller werden für OpenManage Integration for VMware vCenter-Bereitstellungen nicht unterstützt.

Warum wird nach dem Anklicken des Firmware-Links eine Kommunikationsfehlermeldung angezeigt?

Wenn Sie eine langsame Netzwerkverbindung haben (9.600 Bit/s), erhalten Sie eventuell eine Kommunikationsfehlermeldung. Diese wird möglicherweise dann angezeigt, wenn Sie im vSphere-Client auf den Firmware-Link für die OpenManage Integration for VMware vCenter klicken. Dies geschieht, wenn das Zeitlimit für die Verbindung abläuft, während versucht wird, die Liste mit dem Softwarebestand abzurufen. Diese Zeitüberschreitung wird von Microsoft Internet Explorer initiiert. Bei den Versionen 9 und 10 von Microsoft Internet Explorer ist der Wert für die „Zeitüberschreitung beim Empfangen" auf 10 Sekunden voreingestellt. Beheben Sie das Problem, indem Sie die folgenden Schritte durchführen.



Abbildung 5. Firmware-Link-Kommunikationsfehler

1. Öffnen Sie den Microsoft- Registrierungs-Editor (Regedit).
2. Navigieren Sie zum folgenden Ort in der Registrierung:
   KHEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
3. Fügen Sie einen DWORD-Wert für die Zeitüberschreitung beim Empfangen (ReceiveTimeout) hinzu.
4. Setzen Sie den Wert auf 30 Sekunden (30.000) [Möglicherweise muss der Wert für Ihre Umgebung höher eingestellt werden].
5. Beenden Sie Regedit.
6. Starten Sie Internet Explorer neu.

   ANMERKUNG: Es genügt nicht, ein neues Internet Explorer-Fenster zu öffnen. Sie müssen den Internet Explorer-Browser komplett neu starten.

Welche Generation von Dell Servern kann OpenManage Integration for VMware vCenter für SNMP-Traps konfigurieren und unterstützen?

OpenManage Integration for VMware vCenter unterstützt OMSA-SNMP-Traps auf Servern vor der 12. Generation und iDRAC-Traps auf Servern der 12. Generation.

Wie funktioniert die OpenManage Integration for VMware vCenter-Unterstützung von mehr als drei vCenters im verknüpften Modus?

Jedes virtuelle Gerät unterstützt maximal drei vCenters im verknüpften Modus. Wenn Sie über mehr als zehn vCenters verfügen, benötigen Sie für zehn vCenter jeweils eine neue Instanz des Geräts mit entsprechender Lizenzierung.

Unterstützt OpenManage Integration for VMware vCenter vCenter im verknüpften Modus?

Ja, OpenManage Integration for VMware vCenter unterstützt bis zu 10 vCenters im verknüpften Modus. Weitere Informationen über die Funktionsweise von OpenManage Integration for VMware vCenter im verknüpften Modus finden Sie im Whitepaper *Dell Management Plug-in for VMware vCenter: die Arbeit im verknüpften Modus* auf www.Dell.com.

Was sind die für OpenManage Integration for VMware vCenter erforderlichen Port-Einstellungen?



ANMERKUNG: Wenn Sie den OMSA-Agenten über den Link *Probleme auf nicht-konformen vSphere-Hosts beheben* bereitstellen, der im Fenster „Übereinstimmung" im DellManagement Center angezeigt wird, startet das OpenManage Integration for VMware vCenterden httpClient-Dienst und aktiviert Port 8080 bei Versionen nach ESXi 5.0, um OMSA VIB herunterzuladen und zu installieren. Sobald die OMSA-Installation abgeschlossen ist, wird der Dienst automatisch angehalten, und die Schnittstelle wird geschlossen.

Verwenden Sie für das OpenManage Integration for VMware vCenter die folgenden Port-Einstellungen.

Tabelle 3. Schnittstelle virtueller Geräte

Schnittstellennummer	Protokolle	Schnittstellen-Typ	Max. Verschlüsselungsebene	Richtung	Verwendung	Konfigurierbar
21	FTP	TCP	Keine	Ausgang	FTP-Befehls-Client	Nein
53	DNS	TCP	Keine	Ausgang	DNS-Client	Nein
80	HTTP	TCP	Keine	Ausgang	Dell Online-Datenzugriff	Nein
80	HTTP	TCP	Keine	In	Verwaltungskonsole	Nein
162	SNMP-Agent	UDP	Keine	In	SNMP-Agent (Server)	Nein
11620	SNMP-Agent	UDP	Keine	In	SNMP-Agent (Server)	Nein
443	HTTPS	TCP	128–Bit	In	HTTPS-Server	Nein
443	WSMAN	TCP	128–Bit	Ein/Aus	iDRAC/OMSA-Kommunikation	Nein

Schnittstellennummer	Protokolle	Schnittstellen-Typ	Max. Verschlüsselungsebene	Richtung	Verwendung	Konfigurierbar
4433	HTTPS	TCP	128–Bit	In	Automatische Ermittlung	Nein
2049	NFS	UDP	Keine	Alle	Öffentliche Freigabe	Nein
4001–4004	NFS	UDP	Keine	Alle	Öffentliche Freigabe	Nein
11620	SNMP-Agent	UDP	Keine	OM	SNMP-Agent (Server)	Nein

Tabelle 4. Verwaltungsknoten

Schnittstellennummer	Protokolle	Schnittstellen-Typ	Max. Verschlüsselungsebene	Richtung	Verwendung	Konfigurierbar
162, 11620	SNMP	UDP	Keine	Ausgang	Hardware-Ereignisse	Nein
443	WSMAN	TCP	128–Bit	In	iDRAC/OMSA-Kommunikation	Nein
4433	HTTPS	TCP	128–Bit	Ausgang	Automatische Ermittlung	Nein
2049	NFS	UDP	Keine	Alle	Öffentliche Freigabe	Nein
4001–4004	NFS	UDP	Keine	Alle	Öffentliche Freigabe	Nein
443	HTTPS	TCP	128–Bit	In	HTTPS-Server	Nein
8080	HTTP	TCP		In	HTTP-Server; lädt den OMSA VIB herunter und behebt nicht konforme vSphere-Hosts	Nein
50	RMCP	UDP/TCP	128–Bit	Ausgang	Remote Mail Check Protocol	Nein
51	IMP	UDP/TCP	k.A.	k.A.	IMP Logical Address Maintenance	Nein
5353	mDNS	UDP/TCP		Alle	Multicast DNS	Nein
631	IPP	UDP/TCP	Keine	Ausgang	Internet Printing Protocol (IPP)	Nein
69	TFTP	UDP	128–Bit	Alle	Trivial File Transfer (Einfache	Nein

Schnittstellennummer	Protokolle	Schnittstellen-Typ	Max. Verschlüsselungsebene	Richtung	Verwendung	Konfigurierbar
					Dateiübertragung)	
111	NFS	UDP/TCP	128–Bit	In	SUN Remote Procedure Call (Portmap)	Nein
68	BOOTP	UDP	Keine	Ausgang	Bootstrap Protocol Client	Nein

Welche Mindestanforderungen bestehen für die erfolgreiche Installation und den erfolgreichen Betrieb des virtuellen Geräts?

Die folgenden Einstellungen stellen die Mindestanforderungen für das Gerät dar:

- Physischer RAM: 3 GB.
- Reservierter Arbeitsspeicher: 1 GB

  ANMERKUNG: Für optimale Leistung empfiehlt Dell 3 GB.

- Festplatte: 32,5 GB.
- CPU: 2 virtuelle CPUs.

Warum wird das Kennwort für den Benutzer, der für die „Bare-Metal"-Erkennung verwendet wird, nach der erfolgreichen Anwendung des Hardware-Profils, das über den gleichen Benutzer mit neuen geänderten Anmeldeinformationenen in der iDRAC-Benutzer-Liste verfügt, nicht geändert?

Das Kennwort des von der Ermittlung verwendeten Benutzers wird nicht zu den neuen Anmeldeinformationen geändert, wenn nur die Hardware-Profil-Vorlage für die Bereitstellung ausgewählt wird. Dies ist Absicht, so dass das Plugin mit dem iDRAC für eine zukünftige Verwendung in der Bereitstellung kommunizieren kann.

Warum wird in der Ansicht „Prozessor" auf der Seite „System-Überblick" die Prozessor-Version als „Nicht verfügbar" angezeigt?

Im Fall von Dell PowerEdge-Servern der 12. Generation und höher wird die Prozessor-Version in der Marken-Spalte angezeigt. Bei niedrigeren Generation wird die Prozessor-Version in der Versions-Spalte angezeigt.

Warum werden die DNS-Konfigurationseinstellungen nach dem Neustart des Geräts auf die ursprünglichen Einstellungen zurückgesetzt, wenn für die Geräte-IP DHCP verwendet und die DNS-Einstellungen überschrieben werden?

Es ist ein bekannter Fehler, dass statisch zugewiesene DNS-Einstellungen durch die Werte aus dem DHCP ersetzt werden. Das kann vorkommen, wenn DHCP zum Bezug der IP-Einstellungen verwendet wird und DNS-Werte statisch zugewiesen werden. Wenn der DHCP-Lease verlängert oder das System neu gestartet wird, werden die zugewiesenen DNS-Einstellungen entfernt. Lösung: IP-Einstellungen statisch zuweisen, wenn sich die DNS-Servereinstellungen von DHCP unterscheiden.

Betroffene Version: Alle

Warum werden keine Einzelheiten meiner neuen iDRAC-Version auf der Seite der vCenter Hosts & Cluster angezeigt?

Aktualisieren Sie nach der erfolgreichen Fertigstellung einer Firmware-Aktualisierungsaufgabe im Fensterbereich der jüngsten Aufgaben des vSphere Web-Clients die Firmware-Aktualisierungsseite und überprüfen Sie die Firmware-Versionen. Wenn auf der Seite die alten Versionen angezeigt werden, navigieren Sie zur Host-Konformitätsseite in OpenManage Integration for VMware vCenter und prüfen Sie den CISOR-Status dieses Hosts. Wenn CISOR nicht aktiviert ist, aktivieren Sie CISOR und starten Sie den Host neu. Wenn CISOR bereits aktiviert war, melden Sie sich an der iDRAC-Konsole an, setzen Sie den iDRAC zurück, warten Sie einige Minuten und aktualisieren Sie dann die Firmware-Aktualisierungsseite im vSphere-Web-Client.

Wie teste ich Ereigniseinstellungen mithilfe des OMSA, um einen Temperaturfehler an der Hardware zu simulieren?

Gehen Sie wie nachfolgend beschrieben vor, um sicherzustellen, dass die Ereignisse korrekt funktionieren:

1. Navigieren Sie in der OMSA-Benutzeroberfläche zu **Warnungsverwaltung** → **Plattformereignisse**.
2. Aktivieren Sie das Kontrollkästchen **Plattformereignisfilter-Warnungen aktivieren**.
3. Führen Sie einen Bildlauf bis ganz nach unten durch, und klicken Sie auf **Änderungen anwenden**.
4. Um sicherzugehen, dass ein bestimmtes Ereignis aktiviert ist, wie z. B. Temperaturwarnung, wählen Sie aus der Struktur auf der linken Seite die Option **Hauptsystemgehäuse aus**.
5. Wählen Sie unter **Hauptsystemgehäuse Temperaturen** aus.
6. Wählen Sie die Registerkarte **Warnungsverwaltung** und anschließend **Temperatursondenwarnung** aus.
7. Aktivieren Sie das Kontrollkästchen **Broadcast-Übertragung einer Meldung**, und wählen Sie **Änderungen anwenden** aus.
8. Um das Temperaturwarnereignis auszulösen, wählen Sie in der Strukturansicht auf der linken Seite die Option **Hauptsystemgehäuse** aus.
9. Wählen Sie unter **Hauptsystemgehäuse** die Option **Temperaturen** aus.
10. Wählen Sie den Link **Umgebungstemp. der Systemplatine** und dann die Options-Schaltfläche **Auf Werte setzen** aus.
11. Stellen Sie die Option **Maximaler Warnungsschwellenwert** auf einen Wert niedriger als der aktuelle angegebene Messwert ein. Wenn der aktuelle Messwert beispielsweise 27 lautet, stellen Sie den Schwellenwert auf **25**.
12. Wählen Sie **Änderungen anwenden** aus, woraufhin das Temperaturwarnungsereignis generiert wird. Wenn Sie ein weiteres Ereignis auslösen möchten, müssen Sie die ursprünglichen Einstellungen mithilfe der gleichen Option **Auf Werte setzen** wiederherstellen. Die Ereignisse werden als Warnungen generiert und dann auf einen normalen Zustand gesetzt. Wenn alle Vorgänge ordnungsgemäß funktionieren, wechseln Sie zur Ansicht **vCenter-Tasks & -Ereignisse**. Darin sollte keine Temperatursondenwarnung angezeigt werden.

    **ANMERKUNG:** Es gibt einen Filter für doppelte Ereignisse. Wenn Sie versuchen, dasselbe Ereignis zu oft hintereinander auszulösen, erhalten Sie nur ein Ereignis. Um alle Ereignisse anzuzeigen, müssen Sie mindestens 30 Sekunden zwischen dem Auslösen der Ereignisse warten.

Ich habe den OMSA-Agenten auf einem Dell-Hostsystem installiert, es wird jedoch weiterhin eine Fehlermeldung angezeigt, dass OMSA nicht installiert ist. Wie muss ich vorgehen?

Um dieses Problem auf einem Server der 11. Generation zu beheben:

1. Installieren Sie den **OMSA** mit der Komponente **Remote-Aktivierung** auf dem Hostsystem.
2. Wenn Sie den OMSA über die Befehlszeile installieren, müssen Sie die **Option -c** angeben. Wenn der OMSA bereits installiert ist, installieren Sie ihn erneut mit der Option -c, und starten Sie den Dienst neu:

   ```
   srvadmin-install.sh -c srvadmin-services.sh restart
   ```

   Bei einem ESXi-Host müssen Sie **OMSA-VIB** mithilfe des **VMware-Remote-CLI-Tool** installieren, und das System neu starten.

Unterstützt das OpenManage Integration for VMware vCenter ESX/ESXI mit aktiviertem Sperrmodus?

Ja. Der Sperrmodus wird in dieser Version auf den Hosts ESXi 4.1 und höher unterstützt.

Nach einem Neustart tritt bei der Bestandsaufnahme auf den Hosts ESXi 4.0 Update2 und ESXi Update3 im Sperrmodus ein Fehler auf.

Für den Sperrmodus ist ESXi 4.1 oder höher erforderlich. Wenn Sie eine frühere ESXi-Version verwenden und ein Host aus einem beliebigen Grund im Sperrmodus neu gestartet wird, treten bei der Bestandsaufnahme auch weiterhin Fehler auf, sofern Sie nach einem Neustart nicht die folgenden Schritte auf dem Host ausführen.

Schritte für die Problemumgehung bei ESXi 4.0 Update2 und Update3:

1. Klicken Sie unter **vSphere-Client** auf die Option **Hosts und Cluster**, wählen Sie dann im linken Fenster den **Host** aus, und klicken Sie anschließend auf die Registerkarte **Konfiguration**.
2. Klicken Sie im linken Fenster unter **Software** auf **Sicherheitsprofil**.
3. Führen Sie einen Bildlauf bis zu **Sperrmodus** durch, und klicken Sie dann auf **Bearbeiten**.
4. Löschen Sie zum Deaktivieren des Sperrmodus im Dialogfeld **Sperrmodus** das Häkchen im Kontrollkästchen **Aktivieren**, und klicken Sie dann auf **OK**.
5. Melden Sie sich bei der Hostkonsole an, und wählen Sie **Verwaltungs-Agenten neu starten** aus. Drücken Sie die **<EINGABETASTE>** und zum Bestätigen die Taste **<F11>**.
6. Wiederholen Sie zum Aktivieren des Sperrmodus die Schritte 1 bis 4, wählen Sie jedoch diesmal das Kontrollkästchen **Aktivieren** aus, und klicken Sie anschließend auf **OK**.

Beim Verwenden des Sperrmodus ist ein Fehler aufgetreten.

Als ich im Sperrmodus einen Host zum Verbindungsprofil hinzugefügt habe, wurde eine Bestandsaufnahme gestartet, die jedoch mit der Meldung „Es wurde kein Remote Access Controller gefunden, oder auf diesem Host wird keine Bestandsaufnahme unterstützt“ fehlschlug. Die Bestandsaufnahme sollte jedoch für einen Host im Sperrmodus funktionieren, oder?

Wenn Sie den Host in den Sperrmodus versetzen oder einen Host aus dem Sperrmodus entfernen, müssen Sie 30 Minuten warten, bevor Sie den nächsten Vorgang auf dem OpenManage Integration for VMware vCenter durchführen.

Beim Versuch einer Firmware-Aktualisierung mit einer ungültigen DUP fällt der Hardware-Job-Status auf der vCenter-Konsole stundenlang weder aus noch weist er eine Zeitüberschreitung auf. Der Job-Status in LC zeigt aber dennoch „FEHLGESCHLAGEN" an. Warum ist das so?

Wenn die ungültige DUP für die Firmware-Aktualisierung abgerufen wird, bleibt der Status der Aufgabe im vCenter-Konsolen-Fenster auf „In Progress" (In Bearbeitung), die Meldung wird jedoch auf die Ursache des Fehlers geändert. Dies ist ein bekannter Fehler von VMWare und wird in zukünftigen Versionen von VMware vCenter behoben.

Lösung: Die Aufgabe muss manuell abgebrochen werden.

Betroffene Version: Alle

Welche Einstellung sollte ich für UserVars.CIMoeMProviderEnable mit ESXi 4.1 U1 verwenden?

Stellen Sie **UserVars.CIMoemProviderEnabled** auf 1 ein.

Ich habe ein Hardware-Profil mithilfe eines Referenzservers erstellt, es ist jedoch fehlerhaft. Was kann ich tun?

Überprüfen Sie, ob die empfohlenen Mindestversionen der iDRAC- und Lifecycle-Controller-Firmware sowie des BIOS installiert sind.

Um sicherzustellen, dass die vom Referenzserver abgerufenen Daten aktuell sind, müssen Sie die Option **Systembestandsaufnahme beim Neustart sammeln (CSIOR)** aktivieren und den Referenzserver vor der Datenextrahierung neu starten. Lesen Sie den Abschnitt unter Einstellen von CSIOR auf einem Referenzserver.

Ich möchte ESX/ESXi auf einem Blade-Server bereitstellen, dabei tritt jedoch ein Fehler auf. Wie muss ich vorgehen?

Führen Sie folgende Schritte aus, um das Problem zu beheben:

1. Stellen Sie sicher, dass der **ISO-Speicherort (NFS-Pfad)** und die **Stagingordnerpfade** stimmen.
2. Achten Sie darauf, dass sich die während der Zuweisung der Serveridentität ausgewählte **NIC** auf dem gleichen Netzwerk wie das virtuelle Gerät befindet.
3. Falls Sie mit einer **statischen IP-Adresse** arbeiten, müssen Sie sich vergewissern, dass die angegebenen Netzwerkinformationen (einschließlich Subnetzmaske und Standard-Gateway) stimmen. Stellen Sie darüber hinaus sicher, dass die IP-Adresse nicht bereits einem anderen Netzwerk zugewiesen ist.
4. Achten Sie darauf, dass mindestens eine **virtuelle Festplatte** vom System erkannt wird. ESXi kann auch auf einer internen RIPS SD-Karte installiert werden.

Warum schlagen meine Hypervisor-Bereitstellungen auf R210-II-Maschinen fehl?

Ein Zeitüberschreitungsproblem auf R210-II-Maschinen verursacht eine Hypervisor-Bereitstellungs-Fehlermeldung, da das BIOS nicht vom zugehörigen ISO starten kann. Installieren Sie den Hypervisor manuell auf der Maschine, um dieses Problem zu beheben.

Warum werden automatisch erkannte Systeme im Bereitstellungsassistenten ohne Modellinformationen angezeigt?

Meist bedeutet dies, dass die auf dem System installierte Firmware-Version nicht die empfohlenen Mindestanforderungen erfüllt. In einigen Fällen wurde möglicherweise eine Firmware-Aktualisierung nicht auf dem System registriert. Durch einen Kaltstart des Systems oder erneutes Einsetzen des Blades wird dieses Problem behoben. Das neu aktivierte Konto auf dem iDRAC muss deaktiviert und die automatische Erkennung neu initiiert werden, um Modellinformationen und NIC-Informationen für das OpenManage Integration for VMware vCenter bereitzustellen.

Die NFS-Freigabe wurde mit dem ESX/ESXI-ISO eingerichtet, die Bereitstellung schlägt jedoch mit Fehlern beim Laden des Freigabepfads fehl.

Gehen Sie folgendermaßen vor, um die Lösung zu finden:

1. Stellen Sie sicher, dass der iDRAC einen Ping-Befehl an das Gerät senden kann.
2. Stellen Sie außerdem sicher, dass Ihr Netzwerk nicht zu langsam ist.

Wie kann ich die Entfernung des virtuellen Geräts erzwingen?

1. Wechseln Sie zu **https://<vCenter_Server-IP-Adresse>/mob**
2. Geben Sie die VMware vCenter Administrator-Anmeldeinformationen ein.
3. Klicken Sie auf **Inhalt** .
4. Klicken Sie auf **ExtensionManager**.
5. Klicken Sie auf **UnregisterExtension**.
6. Geben Sie den Erweiterungsschlüssel `com.dell.plugin.openManage_integration_for_VMware_vCenter` ein und klicken Sie anschließend auf **Methode aufrufen**.
7. Schalten Sie das virtuelle Gerät OpenManage Integration for VMware vCenter aus und löschen Sie es.

Beim Eingeben eines Kennworts im Bildschirm „Jetzt sichern“ wird eine Fehlermeldung angezeigt.

Wenn Sie einen Monitor mit niedriger Auflösung verwenden, wird das Feld Verschlüsselungskennwort nicht im Fenster JETZT SICHERN angezeigt. Sie müssen auf der Seite einen Bildlauf nach unten durchführen, um das Verschlüsselungskennwort einzugeben.

Bei meiner Firmware-Aktualisierung ist ein Fehler aufgetreten. Wie muss ich vorgehen?

Prüfen Sie in den Protokollen des virtuellen Geräts, ob bei der Aufgabe ein Timeout aufgetreten ist. In diesem Fall muss der iDRAC durch einen kalten Neustart zurückgesetzt werden. Nachdem das System wieder läuft, überprüfen Sie entweder durch Ausführen einer Bestandsaufnahme oder über die Registerkarte „Firmware“, ob die Aktualisierung erfolgreich war.

Meine vCenter-Registrierung ist fehlgeschlagen. Was kann ich tun?

Die vCenter-Registrierung kann aufgrund von Kommunikationsproblemen fehlschlagen. Als Lösung für diese Probleme kann eine statische IP-Adresse verwendet werden. Um eine statische IP-Adresse zu verwenden, wählen Sie auf der Registerkarte „Konsole“ des OpenManage Integration for VMware vCenter die Option **Netzwerk konfigurieren** → **Geräte**

bearbeiten aus, und geben Sie das richtige **Gateway** und den richtigen **FQDN** (vollqualifizierter Domänenname) ein. Geben Sie dann unter „DNS-Konfig bearbeiten" den Namen des DNS-Servers an.

 **ANMERKUNG:** Stellen Sie sicher, dass das virtuelle Gerät den eingegebenen DNS-Server auflösen kann.

Die Leistung ist, während des Tests der Anmeldeinformationen des Verbindungsprofils extrem langsam und die Anwendung reagiert nicht.

Der iDRAC auf einem Server hat nur einen Benutzer (z. B. nur *Stammbenutzer*) und der Benutzer ist deaktiviert oder alle Benutzer befinden sich in einem deaktivierten Zustand. Bei der Kommunikation mit einem Server in einem deaktivierten Zustand kommt es zu Verzögerungen. Um dieses Problem zu beheben, können Sie entweder den deaktivierten Zustand des Servers aufheben oder den iDRAC auf dem Server zurücksetzen, um den Stammbenutzer wieder auf die Standardeinstellung zu aktivieren.

Gehen Sie wie nachfolgend beschrieben vor, um das Problem mit einem Server in einem deaktivierten Zustand zu beheben:

1. Öffnen Sie die Konsole „Chassis Management Controller", und wählen Sie den deaktivierten Server aus.
2. Um die iDRAC-Konsole automatisch zu öffnen, klicken Sie auf **iDRAC-GUI starten**.
3. Navigieren Sie zur Benutzerliste in der iDRAC-Konsole, und wählen Sie eine der folgenden Optionen:
   - iDRAC 6: Wählen Sie die Registerkarten **iDRAC-Einstellungen** → **Netzwerk/Sicherheit** → **Benutzer**.
   - iDRAC 7: Wählen Sie die Registerkarten **iDRAC-Einstellungen** → **Benutzer**.
   - iDRAC 8: Wählen Sie die Registerkarten **iDRAC-Einstellungen** → **Benutzer**.
4. Um die Einstellungen zu bearbeiten, klicken Sie in der Spalte „Benutzer-ID" auf den Link für den Admin-(Stamm-)Benutzer..
5. Klicken Sie auf **Benutzer konfigurieren** und dann auf **Weiter**.
6. Aktivieren Sie auf der Seite „Benutzerkonfiguration" für den ausgewählten Benutzer das Kontrollkästchen neben „Benutzer aktivieren", und klicken Sie dann auf **Anwenden**.

Unterstützt OpenManage Integration for VMware vCenter das VMware vCenter Server-Gerät?

Ja, OpenManage Integration for VMware vCenter unterstützt das VMware vCenter Server-Gerät.

Unterstützt OpenManage Integration for VMware vCenter den vSphere-Web-Client?

Ja, OpenManage Integration for VMware vCenter unterstützt den VMware vSphere-Web-Client.

Warum wird der Aktualisierungs-Repository-Pfad in der Administration Console nicht auf den Standard-Pfad nach dem Zurücksetzen des Geräts auf die werkseitigen Einstellungen eingestellt?

Nachdem Sie das Gerät zurückgesetzt haben, gehen Sie auf die Administration Console und klicken Sie auf der linken Seite auf **GERÄTEVERWALTUNG**. Auf der Seite **Geräteeinstellungen** ist der **Aktualisierungs-Repository-Pfad** nicht auf die Standardeinstellungen zurückgesetzt.

Lösung: Kopieren Sie in der Administration Console manuell den Pfad im Feld **Standard-Aktualisierungs-Repository** in das Feld **Repository-Aktualisierungspfad**.

Warum werden die Alarm-Einstellungen nicht nach der Sicherung und Wiederherstellung von OpenManage Integration for VMware vCenter wiederhergestellt?

Das Wiederherstellen der OpenManage Integration for VMware vCenter-Gerätesicherung stellt nicht alle Alarm-Einstellungen wieder her. Es werden jedoch in der OpenManage Integration for VMware-GUI im Feld **Ereignisse und Alarme** die wiederhergestellten Einstellungen angezeigt.

Lösung: Ändern Sie in OpenManage Integration for VMware-GUI auf der Registerkarte **Verwalten** → **Einstellungen** manuell die Einstellungen für **Ereignisse und Alarme**.

Probleme bei der Bare-Metal-Bereitstellung

In diesem Abschnitt werden Probleme behandelt, die während des Bereitstellungsprozesses auftreten könnten.

Voraussetzungen für Auto-Ermittlung und Handshake

- Bevor Sie Auto-Ermittlung und Handshake ausführen können, müssen Sie sicherstellen, dass die Versionen der iDRAC- und Lifecycle-Controller-Firmware sowie des BIOS die Mindestempfehlungen erfüllen.
- CSIOR muss mindestens einmal auf dem System oder iDRAC ausgeführt worden sein.

Hardware-Konfigurationsfehler

- Achten Sie vor der Initialisierung einer Bereitstellungsaufgabe darauf, dass das System CSIOR abgeschlossen hat und nicht gerade neu gestartet wird.
- Es wird dringend empfohlen, die BIOS-Konfiguration im Klonmodus auszuführen, sodass der Referenzserver ein identisches System ist.
- Manche Controller erlauben keine Erstellung von RAID 0 mit nur einem Laufwerk. Diese Funktion wird nur auf High-End-Controllern unterstützt und die Anwendung solcher Hardwareprofile kann zu Ausfällen führen.

Aktivieren der Auto-Ermittlung auf einem neu erworbenen System

Die Funktion zur Auto-Ermittlung eines Hostsystems ist nicht standardmäßig aktiviert, sondern muss beim Kauf angefordert werden. Wenn die Aktivierung der Auto-Ermittlung zum Zeitpunkt des Kaufs angefordert wird, wird das DHCP auf dem iDRAC aktiviert und Administratorkonten werden deaktiviert. Es muss keine statische IP-Adresse für den iDRAC konfiguriert werden. Er ruft eine solche Adresse von einem DHCP-Server auf dem Netzwerk ab. Um die Funktion zur Auto-Ermittlung nutzen zu können, muss ein DHCP- oder ein DNS-Server (oder beide) konfiguriert werden, um den Ermittlungsprozess zu unterstützen. CSIOR wurde bereits während der Fertigung ausgeführt. Weitere Informationen über die Einrichtung eines Netzwerks zur Unterstützung der Auto-Ermittlung finden Sie in den Dell-Spezifikationen zur Netzwerkeinrichtung für die Auto-Ermittlung unter **http://attachments.wetpaintserv.us/xBUIrs4t%2B2TzbrwqYkblvQ%3D%3D2 62254**

Falls die Auto-Ermittlung nicht zum Zeitpunkt des Kaufs angefordert wurde, kann sie wie folgt aktiviert werden:

1. Drücken Sie während des Startvorgangs <**Strg-E**>.
2. Aktivieren Sie im iDRAC-Setupfenster die NIC (nur Blade-Server).
3. Aktivieren Sie die automatische Ermittlung.
4. Aktivieren Sie DHCP.
5. Deaktivieren Sie die Administratorkonten.
6. Aktivieren Sie **DNS-Serveradresse vom DHCP abrufen**.
7. Aktivieren Sie **DNS-Domänenname vom DHCP abrufen**.
8. Geben Sie in das Feld **Bereitstellungsserver** Folgendes ein:

```
<OpenManage Integration virtual appliance IPaddress>:4433
```

Kontaktaufnahme mit Dell

ANMERKUNG: Wenn Sie nicht über eine aktive Internetverbindung verfügen, können Sie Kontaktinformationen auch auf Ihrer Auftragsbestätigung, dem Lieferschein, der Rechnung oder im Dell-Produktkatalog finden.

Dell stellt verschiedene onlinebasierte und telefonische Support- und Serviceoptionen bereit. Da die Verfügbarkeit dieser Optionen je nach Land und Produkt variiert, stehen einige Services in Ihrer Region möglicherweise nicht zur Verfügung. So erreichen Sie den Vertrieb, den Technischen Support und den Kundendienst von Dell:

1. Besuchen Sie **dell.com/support**.
2. Wählen Sie Ihre Supportkategorie.
3. Wählen Sie das Land bzw. die Region im Listenmenü „Choose a Country/Region“ (Land oder Region auswählen) am oberen Seitenrand aus.
4. Klicken Sie je nach Bedarf auf den entsprechenden Service- oder Support-Link.

OpenManage Integration for VMware vCenter Zugehörige Informationen

- Anzeigen oder Herunterladen von Dell-Serverdokumentation für PowerEdge™-Server unter:
  http://www.dell.com/poweredgemanuals
- Dokumentation zum Dell OpenManage-Systemadministrator
  http:// www.delltechcenter.com/omsa
- Dokumentation zum Dell Lifecycle-Controller
  http://www.dell.com/enterprisemanagement

8

Virtualisierungsbezogene Ereignisse für Dell-PowerEdge-Server

Die folgende Tabelle enthält die kritischen und Warnungsereignisse im Zusammenhang mit der Virtualisierung, einschließlich Name des Ereignisses, Beschreibung und Schweregrad für PowerEdge-Server der 11. und 12. und 13. Generation.

Tabelle 5. Virtualisierungsbezogene Ereignisse von PowerEdge-Servern der 11., 12. und 13. Generation.

Name des Ereignisses	Beschreibung	Schweregrad	Empfohlene Maßnahme
Dell-Current sensor detected a warning value	Ein Stromsensor im angegebenen System hat seinen Warnungsschwellenwert überschritten.	Warnung	Keine Maßnahme
Dell-Current sensor detected a failure value	Ein Stromsensor im angegebenen System hat seinen Fehlerschwellenwert überschritten.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell-Current sensor detected a non-recoverable value	Ein Stromsensor im angegebenen System hat einen Fehler erkannt, der nicht behoben werden kann.	Fehler	Keine Maßnahme
Dell-Redundancy regained	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme
Dell-Redundancy degraded	Ein Redundanzsensor in dem angegebenen System hat erkannt, dass eine der Komponenten der Redundanzeinheit fehlgeschlagen, die Einheit aber dennoch redundant ist.	Warnung	Keine Maßnahme
Dell - Redundancy lost	Ein Redundanzsensor in dem angegebenen System hat erkannt, dass eine der Komponenten in der Redundanzeinheit getrennt wurde, fehlerhaft oder nicht vorhanden ist.	Fehler	Setzen Sie das System in den Wartungsmodus.

Dell - Power supply returned to normal	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme
Dell - Power supply detected a warning	Der Sensormesswert eines Netzteils im angegebenen System hat einen benutzerdefinierbaren Warnungsschwellenwert überschritten.	Warnung	Keine Maßnahme
Dell - Power supply detected a failure	Ein Netzteil wurde abgetrennt oder ist fehlerhaft.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell - Power supply sensor detected a non-recoverable value	Ein Netzteilsensor im angegebenen System hat einen Fehler erkannt, der nicht behoben werden kann.	Fehler	Keine Maßnahme
Dell - Memory Device Status warning	Die Korrekturrate eines Speichergeräts hat einen akzeptierbaren Wert überschritten.	Warnung	Keine Maßnahme
Dell - Memory Device error	Die Korrekturrate eines Speichergeräts hat einen akzeptierbaren Wert überschritten, eine Speicher-Spare-Bank wurde aktiviert oder es ist ein Multibit-ECC-Fehler aufgetreten.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell - Fan enclosure inserted into system	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme
Dell - Fan enclosure removed from system	Ein Lüftergehäuse wurde aus dem angegebenen System entfernt.	Warnung	Keine Maßnahme
Dell - Fan enclosure removed from system for an extended amount of time	Ein Lüftergehäuse wurde für eine vom Benutzer festgelegte Zeitdauer aus dem angegebenen System entfernt.	Fehler	Keine Maßnahme
Dell - Fan enclosure sensor detected a non-recoverable value	Ein Lüftergehäusesensor im angegebenen System hat einen Fehler erkannt, der nicht behoben werden kann.	Fehler	Keine Maßnahme
Dell - AC power has been restored	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme

Dell - AC power has been lost warning	Ein Netzkabel hat seine Leistung verloren, die Redundanz ist jedoch ausreichend, um dies als Warnung zu klassifizieren.	Warnung	Keine Maßnahme
Dell - An AC power cord has lost its power	Ein Netzkabel hat seine Leistung verloren und aufgrund fehlender Redundanz muss dies als Fehler klassifiziert werden.	Fehler	Keine Maßnahme
Dell - Processor sensor returned to a normal value	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme
Dell - Processor sensor detected a warning value	Ein Prozessorsensor im angegebenen System befindet sich in einem gedrosselten Zustand.	Warnung	Keine Maßnahme
Dell - Processor sensor detected a failure value	Ein Prozessorsensor im angegebenen System ist deaktiviert oder bei ihm ist ein Konfigurationsfehler bzw. ein thermischer Auslöser aufgetreten.	Fehler	Keine Maßnahme
Dell - Processor sensor detected a non-recoverable value	Ein Prozessorsensor im angegebenen System ist fehlerhaft.	Fehler	Keine Maßnahme
Dell - Device configuration error	Für ein austauschbares Gerät im angegebenen System wurde ein Konfigurationsfehler erkannt.	Fehler	Keine Maßnahme
Dell - Battery sensor returned to a normal value	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme
Dell - Battery sensor detected a warning value	Ein Batteriesensor im festgelegten System hat erkannt, dass sich ein Akku im vorhersehbaren Fehlerzustand befindet.	Warnung	Keine Maßnahme
Dell - Battery sensor detected a failure value	Ein Batteriesensor im festgelegten System hat erkannt, dass eine Batterie fehlerhaft ist.	Fehler	Keine Maßnahme
Dell - Battery sensor detected a nonrecoverable value	Ein Batteriesensor im festgelegten System hat erkannt, dass eine Batterie fehlerhaft ist.	Fehler	Keine Maßnahme

Dell - Thermal shutdown protection has been initiated	Diese Meldung wird generiert, wenn ein System so konfiguriert wurde, dass es bei einem Fehlerereignis temperaturbedingt herunterfährt. Wenn der Messwert eines Temperatursensors den Fehlerschwellenwert überschreitet, für den das System konfiguriert wurde, fährt das Betriebssystem herunter und das System wird ausgeschaltet. Bei bestimmten Systemen kann dieses Ereignis auch initiiert werden, wenn ein Lüftergehäuse für einen längeren Zeitraum aus dem System entfernt wird.	Fehler	Keine Maßnahme
Dell - Temperature sensor returned to a normal value	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme
Dell - Temperature sensor detected a warning value	Ein Temperatursensor auf der Rückwandplatine, der Systemplatine, der CPU oder dem Festplattenträger im angegebenen System ermittelte ein Überschreiten des Warnungsschwellenwerts.	Warnung	Keine Maßnahme
Dell - Temperature sensor detected a failure value	Ein Temperatursensor auf der Rückwandplatine, der Systemplatine oder dem Festplattenträger im angegebenen System ermittelte ein Überschreiten des Fehlerschwellenwerts.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell - Temperature sensor detected a non-recoverable value	Ein Temperatursensor auf der Rückwandplatine, der Systemplatine oder dem Festplattenträger im angegebenen System erkannte einen Fehler, der nicht behoben werden kann.	Fehler	Keine Maßnahme
Dell - Fan sensor returned to a normal value	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme

Dell - Fan sensor detected a warning value	Ein Lüftersensormesswert in Host <x> hat einen Warnungsschwellenwert überschritten.	Warnung	Keine Maßnahme
Dell - Fan sensor detected a failure value	Ein Lüftersensor im angegebenen System hat den Ausfall eines Lüfters oder mehrerer Lüfter erkannt.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell - Fan sensor detected a nonrecoverable value	Ein Lüftersensor hat einen Fehler erkannt, der nicht behoben werden kann.	Fehler	Keine Maßnahme
Dell - Voltage sensor returned to a normal value	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme
Dell - Voltage sensor detected a warning value	Ein Spannungssensor im angegebenen System hat seinen Warnungsschwellenwert überschritten.	Warnung	Keine Maßnahme
Dell - Voltage sensor detected a failure value	Ein Spannungssensor im angegebenen System hat seinen Fehlerschwellenwert überschritten.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell - Voltage sensor detected a nonrecoverable value	Ein Spannungssensor im angegebenen System hat einen Fehler erkannt, der nicht behoben werden kann.	Fehler	Keine Maßnahme
Dell - Current sensor returned to a normal value	Der Sensor ist auf den Normalwert zurückgekehrt.	Info	Keine Maßnahme
Dell - Storage: storage management error	Die Speicherverwaltung hat einen geräteunabhängigen Fehlerzustand erkannt.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell - Storage: Controller warning	Controller-Warnung. Einzelheiten finden Sie im Register „Aufgaben & Ereignisse“ auf dem vSphere-Client.	Warnung	Keine Maßnahme
Dell - Storage: Controller failure	Controller-Fehler. Einzelheiten finden Sie im Register „Aufgaben & Ereignisse“ auf dem vSphere-Client.	Fehler	Setzen Sie das System in den Wartungsmodus.

Dell - Storage: Channel Failure	Fehler beim Kanal.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell - Storage: Enclosure hardware information	Information zur Gehäuse-Hardware.	Info	Keine Maßnahme
Dell - Storage: Enclosure hardware warning	Warnung bezüglich Gehäuse-Hardware.	Warnung	Keine Maßnahme
Dell - Storage: Enclosure hardware failure	Fehler der Gehäuse-Hardware.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell - Storage: Array disk failure	Fehler der Array-Festplatte.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell - Storage: EMM failure	EMM-Fehler.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell - Storage: power supply failure	Netzteilfehler.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell - Storage: temperature probe warning	Temperatursondenwarnung der physischen Festplatte: zu kalt oder zu heiß.	Warnung	Keine Maßnahme
Dell - Storage: temperature probe failure	Temperatursondenfehler der physischen Festplatte: zu kalt oder zu heiß.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell - Storage: Fan failure	Lüfterfehler.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell - Storage: Battery warning	Batteriewarnung.	Warnung	Keine Maßnahme
Dell - Storage: Virtual disk degraded warning	Warnung zur Herabsetzung einer virtuellen Festplatte.	Warnung	Keine Maßnahme
Dell - Storage: Virtual disk degraded failure	Fehler zur Herabsetzung einer virtuellen Festplatte.	Fehler	Setzen Sie das System in den Wartungsmodus.
Dell - Storage: Temperature probe information	Informationen zur Temperatursonde	Info	Keine Maßnahme
Dell - Storage: Array disk warning	Warnung zur Array-Festplatte.	Warnung	Keine Maßnahme
Dell - Storage: Array disk information	Informationen zur Array-Festplatte.	Info	Keine Maßnahme
Dell - Storage: Power supply warning	Netzteilwarnung.	Warnung	Keine Maßnahme
Dell - Chassis Intrusion - Physical Security Violation	Gehäuseeingriff – Physische Sicherheitsverletzung	Fehler	Keine Maßnahme

Dell - Chassis Intrusion(Physical Security Violation) Event Cleared	Das Ereignis Gehäuseeingriff (physische Sicherheitsverletzung) wurde gelöscht.	info	Keine Maßnahme
Dell - CPU Presence (Processor Presence detected)	CPU-Anwesenheit (Prozessor-Anwesenheit ermittelt)	info	Keine Maßnahme
Dell - System Event Log (SEL) Full (Logging Disabled)	Das Systemereignisprotokoll (SEL) ist voll (Protokollierung deaktiviert)	Fehler	Keine Maßnahme
Dell - System Event Log (SEL) Cleared	Das Systemereignisprotokoll (SEL) wurde gelöscht.	info	Keine Maßnahme
Dell - SD Card redundancy Has Returned to Normal	Die Redundanz der SD-Karte ist wieder normal.	info	Keine Maßnahme
Dell - SD Card Redundancy has been Lost	Die Redundanz der SD-Karte ist nicht mehr vorhanden.	Fehler	Keine Maßnahme
Dell - SD Card Redundancy Degraded	Die Redundanz der SD-Karte ist herabgesetzt.	Warnung	Keine Maßnahme
Dell - Module SD Card Present (SD Card Presence Detected)	Eine Modul-SD-Karte ist vorhanden (Anwesenheit SD-Karte ermittelt).	info	Keine Maßnahme
Dell - Module SD Card Failed (Error)	Die Modul-SD-Karte ist fehlerhaft (Fehler).	Fehler	Keine Maßnahme
Dell - Module SD Card Write Protect(Warning)	Die Modul-SD-Karte ist schreibgeschützt (Warnung).	Warnung	Keine Maßnahme
Dell - Module SD Card not Present	Die Modul-SD-Karte ist nicht vorhanden.	info	Keine Maßnahme
Dell - Watchdog Timer Expired	Der Watchdog-Zeitgeber ist abgelaufen.	Fehler	Keine Maßnahme
Dell - Watchdog Reset	Watchdog-Reset	Fehler	Keine Maßnahme
Dell - Watchdog Power Down	Watchdog herunterfahren	Fehler	Keine Maßnahme
Dell - Watchdog Power cycle	Watchdog aus- und einschalten	Fehler	Keine Maßnahme
Dell - System Power Exceeds PSU Wattage	Der Systemstrom liegt über der PSU-Wattleistung.	Fehler	Keine Maßnahme

Dell - System Power Exceeds Error Cleared	Der Fehler wegen hohem Systemstrom wurde gelöscht.	info	Keine Maßnahme
Dell - Power Supply Inserted	Das Netzteil ist eingesetzt.	info	Keine Maßnahme
Dell - Internal Dual SD Module is present	Das interne Dual SD-Modul ist vorhanden.	info	Keine Maßnahme
Dell - Internal Dual SD Module is online	Das interne Dual SD-Modul ist online.	info	Keine Maßnahme
Dell - Internal Dual SD Module is operating normally	Das interne Dual SD-Modul funktioniert normal.	info	Keine Maßnahme
Dell - Internal Dual SD Module is write protected	Das interne Dual SD-Modul ist schreibgeschützt.	Warnung	Keine Maßnahme
Dell - Internal Dual SD Module is writable	Das interne Dual SD-Modul ist beschreibbar.	info	Keine Maßnahme
Dell - Integrated Dual SD Module is absent	Das integrierte Dual SD-Modul ist nicht vorhanden.	Fehler	Keine Maßnahme
Dell - Integrated Dual SD Module redundancy is lost	Die Redundanz des integrierten Dual SD-Moduls ist nicht mehr vorhanden.	Fehler	Keine Maßnahme
Dell - Internal Dual SD Module is redundant	Das interne Dual SD-Modul ist redundant.	info	Keine Maßnahme
Dell - Internal Dual SD Module is not redundant	Das interne Dual SD-Modul ist nicht redundant.	info	Keine Maßnahme
Dell - Integrated Dual SD Module failure	Es liegt ein Fehler am integrierten Dual SD-Modul vor.	Fehler	Keine Maßnahme
Dell - Internal Dual SD Module is offline	Das interne Dual SD-Modul ist offline.	Warnung	Keine Maßnahme
Dell - Integrated Dual SD Module redundancy is degraded	Die Redundanz des integrierten Dual SD-Moduls ist herabgesetzt.	Warnung	Keine Maßnahme
Dell - SD card device has detected a warning	Das SD-Kartengerät hat eine Warnung erkannt.	Warnung	Keine Maßnahme
Dell - SD card device has detected a failure	Das SD-Kartengerät hat einen Fehler erkannt.	Fehler	Keine Maßnahme
Dell - Integrated Dual SD Module warning	Es liegt eine Warnung für das integrierte Dual SD-Modul vor.	Warnung	Keine Maßnahme

Dell - Integrated Dual SD Module information	Es liegen Informationen zum integrierten Dual SD-Modul vor.	info	Keine Maßnahme
Dell - Integrated Dual SD Module redundancy information	Es liegen Informationen zur Redundanz des integrierten Dual SD-Moduls vor.	info	Keine Maßnahme
Dell - Network failure or critical event	Es liegt ein Netzwerkfehler oder ein kritisches Ereignis vor.	Fehler	Keine Maßnahme
Dell - Network warning	Netzwerkwarnung	Warnung	Keine Maßnahme
Dell - Network information	Netzwerkinformationen	info	Keine Maßnahme
Dell - Physical disk failure	Es liegt ein Fehler an der physischen Festplatte vor.	Fehler	Keine Maßnahme
Dell - Physical disk warning	Es liegt eine Warnung für die physische Festplatte vor.	Warnung	Keine Maßnahme
Dell - Physical disk information	Es liegen Informationen zur physischen Festplatte vor.	info	Keine Maßnahme
Dell - An error was detected for a PCI device	Es wurde ein Fehler am PCI-Gerät erkannt.	Fehler	Keine Maßnahme
Dell - A warning event was detected for a PCI device	Es wurde ein Warnungsereignis für ein PCI-Gerät erkannt.	Warnung	Keine Maßnahme
Dell - An informational event was detected for a PCI device	Es wurde ein Informationsereignis für ein PCI-Gerät erkannt.	info	Keine Maßnahme



Grundlegendes zur automatischen Ermittlung

Die automatische Ermittlung ist ein Prozess, bei dem ein Dell PowerEdge-Bare-Metal-Server der 11., 12. oder 13. Generation zu einem Pool verfügbarer Server hinzugefügt wird, damit er von OpenManage Integration for VMware vCenter verwendet werden kann. Nachdem ein Server ermittelt wurde, können Sie ihn für die Hypervisor- und Hardware-Bereitstellung verwenden. In diesem Anhang finden Sie alle Informationen zur automatischen Ermittlung, die Sie für die Systemkonfiguration benötigen. Die automatische Ermittlung ist eine Lifecycle Controller-Funktion zum Einrichten und Registrieren eines neuen Servers mithilfe einer Konsole. Zu den Vorteilen dieser Funktion gehört zum einen, dass keine umständliche manuelle lokale Konfiguration des neuen Servers erforderlich ist, und zum anderen, dass ein neuer Server, nachdem er mit dem Netzwerk verbunden und an die Stromversorgung angeschlossen wurde, automatisch von der Konsole ermittelt wird.

Die automatische Ermittlung wird aufgrund der durchgeführten Prozesse auch als *Ermittlung und Handshake* bezeichnet. Wenn ein neuer Server mit aktivierter automatischer Ermittlung an die Stromversorgung angeschlossen und mit einem Netzwerk verbunden ist, versucht der Lifecycle Controller des Dell Servers, eine Bereitstellungskonsole zu *ermitteln*, die im Dell Bereitstellungsserver integriert ist. Die automatische Ermittlungsfunktion leitet dann einen sogenannten *Handshake* zwischen dem Bereitstellungsserver und dem Lifecycle Controller ein.

OpenManage Integration for VMware vCenter ist eine Bereitstellungskonsole mit integriertem Bereitstellungsserver. Der Speicherort des Bereitstellungsservers wird dem iDRAC auf unterschiedliche Weise mitgeteilt. Die IP-Adresse oder der Host-Name für den Speicherort des Bereitstellungsservers wird mit der IP-Adresse oder dem Host-Namen der virtuellen Maschine des OpenManage Integration for VMware vCenter-Geräts gleichgesetzt.



ANMERKUNG: Ein neuer Server, der für die automatische Ermittlung konfiguriert ist, versucht in einem Zeitraum von 24 Stunden alle 90 Sekunden, den Speicherort des Bereitstellungsservers aufzulösen. Nach diesem Zeitraum können Sie die automatische Ermittlung manuell erneut einleiten.

Beim Empfang der Anforderung für die automatische Ermittlung durch OpenManage Integration for VMware vCenter wird das SSL-Zertifikat validiert. Anschließend werden etwaige optional konfigurierte Sicherheitsverfahren eingeleitet, z. B. Abruf Client-seitiger Sicherheitszertifikate und Abgleich mit einer Whitelist. Anhand einer zweiten Validierungsanforderung seitens des neuen Servers werden die vorläufigen Anmeldeinformationen (Benutzername und Kennwort) ausgegeben, die auf dem iDRAC konfiguriert werden sollen. Anschließend werden von OpenManage Integration for VMware vCenter weitere Aufrufe initiiert. Dabei werden Informationen zum Server erfasst, die vorläufigen Anmeldeinformationen entfernt und dauerhafte benutzerdefinierte Anmeldeinformationen für den Verwaltungszugriff konfiguriert.

Wenn die automatische Ermittlung erfolgreich war, werden die zum Zeitpunkt der Ermittlung auf der Seite **Einstellungen** → **Bereitstellung** vorhandenen Anmeldeinformationen auf dem Ziel-iDRAC erstellt. Anschließend wird die automatische Ermittlung deaktiviert. Der Server müsste jetzt im Pool der verfügbaren Bare-Metal-Server unter „Bereitstellung“ in OpenManage Integration for VMware vCenter angezeigt werden.

Die automatische Ermittlung kann zurzeit über den vSphere Desktop-Client erfolgen.

Voraussetzungen für die automatische Ermittlung

Bevor Sie versuchen Dell PowerEdge-Bare-Metal-Server der 11., 12. oder späteren Generation zu ermitteln, installieren Sie OpenManage Integration for VMware vCenter. Nur Dell PowerEdge-Server ab der 11. Generation mit iDRAC-Express oder iDRAC-Enterprise können im OpenManage Integration for VMware vCenter-Pool der Bare-Metal-Server ermittelt

werden. Es ist eine Netzwerkkonnektivität zwischen dem iDRAC des Dell Bare-Metal-Servers und der virtuellen Maschine des OpenManage Integration for VMware vCenter erforderlich.



ANMERKUNG: Hosts mit bereits vorhandenen Hypervisor sollten nicht durch das OpenManage Integration for VMware vCenter-Plugin ermittelt werden. Fügen Sie den Hypervisor stattdessen zu einem Verbindungsprofil hinzu und gleichen Sie ihn anschließend mithilfe des Assistenten für Host-Kompatibilität an das OpenManage Integration for VMware vCenter an.

Damit eine automatische Ermittlung stattfinden kann, müssen die folgenden Voraussetzungen erfüllt sein:

- **Strom:** Schließen Sie den Server an die Stromversorgung an. Der Server muss jedoch nicht eingeschaltet werden.
- **Netzwerkkonnektivität:** Der iDRAC des Servers muss über Netzwerkkonnektivität verfügen und über Port 4433 mit dem Bereitstellungsserver kommunizieren. Sie können die IP-Adresse über einen DHCP-Server anfordern oder diese manuell im iDRAC-Konfigurationshilfsprogramm angeben.
- **Zusätzliche Netzwerkeinstellungen:** Aktivieren Sie bei Verwendung von DHCP die Einstellung *DNS-Serveradresse über DHCP anfordern*, damit eine DNS-Namensauflösung erfolgen kann.
- **Speicherort des Bereitstellungsdienstes:** Dem iDRAC muss die IP-Adresse oder der Host-Name des Servers mit dem Bereitstellungsdienst bekannt sein.
- **Kontozugriff deaktiviert:** Aktivieren Sie den Zugriff des Verwaltungskontos auf den iDRAC. Falls iDRAC-Konten mit Administratorrechten vorhanden sind, müssen Sie diese zuerst über die iDRAC-Webkonsole deaktivieren. Nachdem die automatische Ermittlung erfolgreich durchgeführt wurde, wird das iDRAC-Verwaltungskonto wieder aktiviert.
- **Automatische Ermittlung aktiviert:** Auf dem iDRAC des Servers muss die Funktion für die automatische Ermittlung aktiviert sein, damit die automatische Ermittlung starten kann.

Aktivieren und Deaktivieren von Verwaltungskonten auf iDRAC-Servern

Damit Sie die automatische Ermittlung einrichten können, müssen Sie zuerst alle Verwaltungskonten, mit Ausnahme des Stammkontos, deaktivieren. Das Stammkonto wird im Rahmen der automatischen Ermittlung deaktiviert. Nachdem Sie die automatische Ermittlung erfolgreich eingerichtet haben, kehren Sie zurück zur GUI von Integrated Dell Remote Access Controller 6, und aktivieren Sie die Konten wieder, die Sie zuvor deaktiviert haben. Dieses Verfahren gilt für PowerEdge-Server der 11., 12. und 13. Generation.



ANMERKUNG: Als Schutzmaßnahme für den Fall des Fehlschlagens der automatischen Ermittlung können Sie ein Konto auf dem iDRAC aktivieren, das kein Verwaltungskonto ist. Auf diese Weise verfügen Sie über die Möglichkeit eines Remote-Zugriffs, falls die automatische Ermittlung fehlschlägt.

1. Geben Sie die **iDRAC-IP-Adresse** in einen Browser ein.
2. Melden Sie sich an der **GUI von Integrated Dell Remote Access Controller** an.
3. Führen Sie einen der folgenden Vorgänge aus:
   - Bei iDRAC6: Wählen Sie im linken Fenster **iDRAC-Einstellungen** → **Netzwerk/Sicherheit** → **Benutzer** aus.
   - Bei iDRAC7: Wählen Sie im linken Fenster **iDRAC-Einstellungen** → **Benutzerauthentifizierung** → **Benutzer** aus.
4. Machen Sie im Register „Benutzer“ alle Verwaltungskonten ausfindig, bei denen es sich nicht um das Stammkonto handelt.
5. Wählen Sie zum Deaktivieren eines Kontos unter „Benutzer-ID“ die entsprechende **ID** aus.
6. Klicken Sie auf **Weiter.**
7. Heben Sie auf der Seite „Benutzerkonfiguration“ unter „Allgemein“ die Markierung des Kontrollkästchens **Benutzer aktivieren** auf.
8. Klicken Sie auf **Anwenden**.

9. Nachdem Sie die automatische Ermittlung erfolgreich eingerichtet haben, müssen Sie die einzelnen Konten wieder aktivieren. Wiederholen Sie dazu die Schritte 1 bis 8, wobei Sie jedoch diesmal das Kontrollkästchen **Benutzer aktivieren** markieren und anschließend auf **Anwenden** klicken.

Manuelles Konfigurieren eines Servers für Auto-Ermittlung (11. Generation von PowerEdge-Servern)

Sie müssen über die iDRAC- und die Host-IP-Adresse verfügen.
Falls Sie Ihr Bare-Metal-Gerät nicht bereits mit werkseitiger Konfiguration für die automatische Ermittlung bestellt haben, können Sie die Funktion auch manuell einrichten. iDRAC verfügt über zwei Benutzerschnittstellen, die beide über die IP-Adresse des einzurichtenden iDRAC erreichbar sind.

Bei erfolgreicher automatischer Ermittlung der Bare-Metal-Server wird das neue Verwaltungskonto erstellt bzw. ein vorhandenes Konto mit den vom Handshake-Dienst übergebenen Anmeldeinformationen aktiviert. Alle anderen Verwaltungskonten, die vor der automatischen Ermittlung deaktiviert wurden, werden nicht automatisch wieder aktiviert. Sie müssen diese nach erfolgreichem Abschluss der automatischen Ermittlung selbst wieder aktivieren. Lesen Sie dazu den Abschnitt Aktivieren und Deaktivieren von Verwaltungskonten auf iDRAC-Servern.



ANMERKUNG: Falls die automatische Ermittlung aus irgendeinem Grund nicht vollständig durchgeführt wurde, gibt es primär keine Möglichkeit, eine Remote-Verbindung zum iDRAC herzustellen. Sie können eine solche Remote-Verbindung nur dann herstellen, wenn Sie auf dem iDRAC ein Konto aktiviert haben, das kein Verwaltungskonto ist. Falls auf dem iDRAC kein aktiviertes Konto vorhanden ist, können Sie nur auf den iDRAC zugreifen, indem Sie sich lokal am Gerät anmelden und das Konto auf dem iDRAC aktivieren.

1. Geben Sie die **iDRAC-IP**-Adresse in einen Browser ein.
2. Melden Sie sich an der **GUI von iDRAC Enterprise** an.
3. Klicken Sie in der Registerkarte **Integrated Dell Remote Access Controller 6 – Enterprise** → **Zusammenfassung** in der Vorschau der virtuellen Konsole auf **Starten**.
4. Klicken Sie im Dialogfeld „Warnung – Sicherheit“ auf **Ja**.
5. Drücken Sie in der iDRAC-Programmkonsole einmal oder zweimal auf **F12**, um das Dialogfeld „Authentifizierung erforderlich“ aufzurufen.
6. Im Dialogfeld „Authentifizierung erforderlich“ wird der Name angezeigt. Drücken Sie die **Eingabetaste**.
7. Geben Sie Ihr **Kennwort** ein.
8. Drücken Sie die **Eingabetaste.**
9. Wenn das Dialogfeld „Herunterfahren/Neustart“ angezeigt wird, drücken Sie auf **F11**.
10. Der Host wird neu gestartet und der Bildschirm zeigt Informationen zum Laden des Speichers und dann zu RAID an. Wenn iDRAC angezeigt wird und Sie aufgefordert werden, die Tastenkombination STRG + E zu drücken, drücken Sie unverzüglich auf **STRG + E**.

    Wenn dieses Dialogfeld angezeigt wird, war Ihre Aktion erfolgreich. Wechseln Sie anderenfalls in das Menü „Strom“, schalten Sie das System aus und wieder ein, und wiederholen Sie den Vorgang.

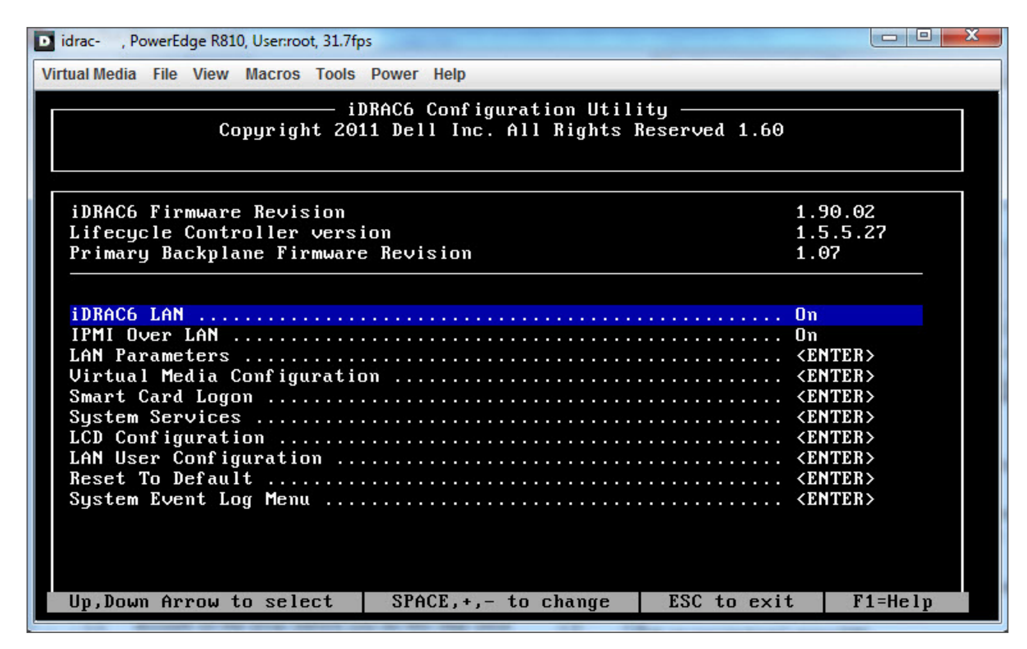


Abbildung 6. Drücken Sie die Tastenkombination STRG + E, um diesen Bildschirm zu aktivieren.

11. Markieren Sie im iDRAC6-Konfigurationshilfsprogramm mithilfe der Pfeiltasten die Option **LAN-Parameter**.
12. Drücken Sie die **Eingabetaste**.
13. Falls es sich bei diesem Host um ein Blade-System handelt, verwenden Sie zum Konfigurieren der NIC die Leertaste, um die Optionen auf **Aktiviert** zu setzen.
14. Wählen Sie bei Verwendung von DHCP mithilfe der Pfeiltasten die Option **Domänenname über DHCP** aus.
15. Setzen Sie die Option mithilfe der Leertaste auf **Eingeschaltet**.
16. Wechseln Sie bei Verwendung von DHCP mithilfe der Pfeiltasten zu den IPv4-Einstellungen, und markieren Sie die Option **DNS-Server über DHCP**.
17. Setzen Sie die Option mithilfe der Leertaste auf **Eingeschaltet**.
18. Drücken Sie zum Beenden die Taste **Esc** auf Ihrer Tastatur.
19. Markieren Sie mithilfe der Pfeiltasten die Option **LAN-Benutzerkonfiguration**.
20. Markieren Sie mithilfe der Pfeiltasten die Option **Bereitstellungsserver**.
21. Drücken Sie die **Eingabetaste**.
22. Geben Sie die IP-Adresse des Hosts ein.
23. Drücken Sie erneut auf **Esc**.
24. Markieren Sie mithilfe der Pfeiltasten die Option **Kontozugriff**.
25. Setzen Sie die Option mithilfe der Leertaste auf **Deaktivieren**.
26. Markieren Sie mithilfe der Pfeiltasten die Option **Automatische Ermittlung**.
27. Setzen Sie die Option mithilfe der Leertaste auf **Aktiviert**.
28. Drücken Sie auf Ihrer Tastatur auf **Esc**.
29. Drücken Sie ein zweites Mal auf **Esc**.

Manuelles Konfigurieren eines Servers für die Auto-Ermittlung (12. Generation von PowerEdge-Servern)

Sie müssen über die iDRAC- und die Host-IP-Adresse verfügen.

Falls Sie Ihr Bare-Metal-Gerät nicht bereits mit werkseitiger Konfiguration für die automatische Ermittlung bestellt haben, können Sie die Funktion auch manuell einrichten. iDRAC verfügt über zwei Benutzerschnittstellen, die beide über die IP-Adresse des einzurichtenden iDRAC erreichbar sind.

Bei erfolgreicher automatischer Ermittlung der Bare-Metal-Server wird das neue Verwaltungskonto erstellt bzw. ein vorhandenes Konto mit den vom Handshake-Dienst übergebenen Anmeldeinformationen aktiviert. Alle anderen Verwaltungskonten, die vor der automatischen Ermittlung deaktiviert wurden, werden nicht automatisch wieder aktiviert. Sie müssen diese nach erfolgreichem Abschluss der automatischen Ermittlung selbst wieder aktivieren. Lesen Sie dazu den Abschnitt Aktivieren und Deaktivieren von Verwaltungskonten auf iDRAC-Servern.



ANMERKUNG: Falls die automatische Ermittlung aus irgendeinem Grund nicht vollständig durchgeführt wurde, gibt es primär keine Möglichkeit, eine Remote-Verbindung zum iDRAC herzustellen. Sie können eine solche Remote-Verbindung nur dann herstellen, wenn Sie auf dem iDRAC ein Konto aktiviert haben, das kein Verwaltungskonto ist. Falls auf dem iDRAC kein aktiviertes Konto vorhanden ist, können Sie nur auf den iDRAC zugreifen, indem Sie sich lokal am Gerät anmelden und das Konto auf dem iDRAC aktivieren.

1. Geben Sie die **iDRAC-IP-Adresse** in einen Browser ein.
2. Melden Sie sich an der **GUI von iDRAC Enterprise** an.
3. Klicken Sie in der Registerkarte **Integrated Dell Remote Access Controller 7 – Enterprise** → **Zusammenfassung** in der Vorschau der virtuellen Konsole auf **Starten**.
4. Klicken Sie im Dialogfeld „Warnung – Sicherheit" auf **Ja**.
5. Drücken Sie in der iDRAC-Programmkonsole einmal oder zweimal auf **F12**, um das Dialogfeld „Authentifizierung erforderlich" aufzurufen.
6. Im Dialogfeld „Authentifizierung erforderlich" wird der Name angezeigt. Drücken Sie die **Eingabetaste**.
7. Geben Sie Ihr **Kennwort** ein.
8. Drücken Sie die **Eingabetaste.**
9. Wenn das Dialogfeld „Herunterfahren/Neustart" angezeigt wird, drücken Sie auf **F11**.
10. Der Host wird neu gestartet und der Bildschirm zeigt Informationen zum Laden des Speichers und dann zu RAID an. Wenn ein Dell Bildschirm angezeigt wird, in dem Sie aufgefordert werden, die Taste F2 zu drücken, drücken Sie unverzüglich auf **F2**.

    Warten Sie, bis der Dell System-Setup-Bildschirm angezeigt wird. Dies kann einige Minuten dauern.
11. Markieren Sie im Dell System-Setup-Bildschirm mithilfe der Pfeiltasten die Option **iDRAC-Einstellungen**.
12. Markieren Sie mithilfe der Pfeiltasten die Option **Remote-Aktivierung**.
13. Klicken Sie zum Aktivieren der automatischen Ermittlung auf **Aktivieren**.
14. Drücken Sie auf **Esc**.
15. Drücken Sie erneut auf **Esc**.
16. Klicken Sie im Warnungsbildschirm auf **Ja**, um den Vorgang des Beendens zu bestätigen.